MASTER'S THESIS

De differentiatie tussen hoofdkantoor en bijkantoor en het effect op het bewustzijn van informatiebeveiliging binnen een financiële instelling

van Paassen, S. (Sandra)

Award date:
2021

Master Thesis

De differentiatie tussen hoofdkantoor en bijkantoor en het effect op het bewustzijn van informatiebeveiliging binnen een financiële instelling

Opleiding:	Open Universiteit, Bètawetenschappen Masteropleiding Business Process Management & IT
Programma:	Open University of the Netherlands, Faculty of Science Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeeropdracht Business Process Management and IT
Student:	Sandra van Paassen
Identiteitsnummer:	
Datum:	07-02-2021
Afstudeerbegeleider	Prof. Dr. A. Bijlsma
Tweede lezer	Dr. L.W. Rutledge
Versie nummer:	1.0
Status:	Definitief

Abstract

Information Security Awareness (ISA) wordt gezien als de mate waarin elke medewerker het belang van informatiebeveiliging begrijpt, de niveaus van informatiebeveiliging die geschikt zijn voor de organisatie, hun individuele beveiligingsverantwoordelijkheden en handelt hiernaar. Uit een onderzoek naar ISA binnen 3 grootbanken blijkt dat er differentiatie in groepen is gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers. Over het algemeen zijn de medewerkers op een hoofdkantoor gefocust op het algemene beheer van een bank zonder klantcontact. De medewerkers op een bijkantoor hebben wel direct klantencontact. Deze onderscheidende profielen hebben sterke implicaties voor het beveiligingsgedrag. Uit eerder onderzoek zijn een aantal verschillen tussen de groepen medewerkers waargenomen, om deze resultaten te generaliseren en de betrouwbaarheid te verhogen is binnen dezelfde grootbank gebruik gemaakt van dezelfde enquête genaamd HAIS-Q. Dit heeft geresulteerd in een aantal waarnemingen die gebruikt kunnen worden voor toekomstig onderzoek.

Sleutelbegrippen

Information security awareness, Security awareness, Cyber awareness, Beveiligingsbewustzijn, Bank employees

Samenvatting

Binnen de financiële dienstverlening wordt veelvoudig gevoelige klantinformatie opgeslagen, overgedragen en verzameld. Terwijl informatiebeveiliging in het algemeen gericht is op het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, gaat het bewust omgaan met informatiebeveiliging om het creëren en behouden van beveiligingsgedrag als kritisch element in een effectieve informatiebeveiligingsomgeving, ofwel afgekort: ISA. Uit literatuuronderzoek is gebleken dat ondanks het gebruik van meerdere controles organisaties beveiligingslekken blijven ervaren, er tekortkomingen zijn in bewustwordingsgedrag en beveiligingsbewustzijn van medewerkers de grootste uitdaging betreft. Uit een onderzoek naar ISA binnen 3 grootbanken bleek dat er differentiatie in groepen is gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers echter is de inhoud van de differentiatie niet onderzocht.

Om nieuwe kennis aan de bestaande kennis toe te voegen wordt er naar antwoord gezocht op de volgende hoofdvraag: ***"Wat heeft een differentiatie op ISA voor effect op de informatiebeveiliging van hoofd- en bijkantoor?"*** Om dit antwoord te achterhalen is er gestart met een literatuur onderzoek gevolgd door empirisch onderzoek. Middels zes deelvragen gaat dit onderzoek in op een aanvulling op belangrijke aspecten van ISA, welke factoren omtrent ISA een belangrijke rol binnen de financiële dienstverlening spelen, de verschillen van ISA tussen medewerkers van het hoofdkantoor en bijkantoor, welke factoren van invloed zijn op informatiebeveiligingsgedrag, welke bewustmakingscampagnes eventueel kunnen bijdragen aan ISA en tot slot antwoord op de vraag of een ISA-programma wordt beïnvloed door de verschillen tussen medewerkers van het hoofdkantoor en de medewerkers van een bijkantoor. Het theoretische deel gaat in op de bestaande literatuur, het empirische deel van het onderzoek gaat in op de toetsing van deze literatuur. De zogenaamde toetsing en daadwerkelijke uitvoering van het onderzoek wordt gedaan middels een case study, enkelvoudig embedded design uitgevoerd binnen een van de drie grootbanken in Nederland. De case als geheel bestaat uit meerdere elementen doordat het verschil wordt onderzocht tussen de medewerkers van een bijkantoor en het hoofdkantoor. De onderzoeksmethode wordt vormgegeven middels een enquête gebaseerd op de HAIS-Q en is ingezet binnen zowel het hoofdkantoor als binnen de bijkantoren. Hierbij wordt rekening gehouden met een eerder onderzoek binnen bank X, tevens gehouden omtrent het onderwerp ISA.

In totaal hebben 87 van de 468 medewerkers de enquête ingevuld waarvan 60 volledig en 27 onvolledig. Uit de resultaten zijn interessante significante verschillen waargenomen tussen de medewerkers van een lokaal kantoor en medewerkers van een bijkantoor. Voor het aandachtsgebied Password Management zien de we de volgende significante verschillen: "It's safe to use the same password for social media and work accounts": medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) scoren hoger dan de medewerkers van een bijkantoor. Daarnaast geeft de test weer dat de medewerkers van een bijkantoor (op de KAB dimensie Attitude) hoger scoren dan de medewerkers van het hoofdkantoor op het volgende item: "It's a bad idea to share my work passwords, even if a colleague asks for it". Voor het aandachtsgebied Social Media use zien we het volgende significante verschil: "It's risky to post certain information about my work on social media": medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) scoren hoger dan de medewerkers van een bijkantoor.

Een belangrijke bevinding in dit onderzoek betreft een gelijk ISA niveau tussen de twee groepen medewerkers. Daarnaast wordt de theorie bevestigd doordat uit het resultaat blijkt dat medewerkers van het hoofdkantoor een hoger ISA niveau voor het aandachtsgebied wachtwoordbeheer hebben dan de medewerkers van een bijkantoor. Opvallend is wel dat de significante verschillen niet op dezelfde items uit eerder onderzoek zijn geconstateerd. Daarnaast zijn er geen belangrijke verschillen in het aandachtsgebied e-mail gebruik geconstateerd, een beperking uit vorig onderzoek was dat er geen inzicht was in de mate waarin de respondenten

contact hadden met onbekende afzenders en de aanname is gedaan dat medewerkers van een bijkantoor vaker contact met onbekende afzenders heeft. Uit ons resultaat blijkt dat 17 van de 45 medewerkers van het hoofdkantoor contact heeft met onbekende afzenders tegenover 28 medewerkers van een bijkantoor. Het aandachtsgebied social media geeft een gelijk niveau van ISA tussen de verschillende groepen weer, daarnaast is er wel een significant verschil geconstateerd op een ander item dan de items op het gebied van social media in eerder onderzoek. Op basis van dit item kan er geconcludeerd worden dat de medewerkers van een bijkantoor het minder risicovol vinden om bepaalde informatie over werk op social media te plaatsen.

Met de nieuwe inzichten kan er geconcludeerd worden dat de verschillen tussen de groepen medewerkers binnen grootbank X kleiner zijn dan eerste instantie werd gedacht. Deze conclusie is dan puur gebaseerd op resultaat uit de statistische toetsen waaruit minder significante verschillen op item niveau zijn geconstateerd. Echter is een sample van 60 respondenten te laag om een uitspraak over de gehele populatie te kunnen doen. Om de exacte oorzaak van deze verschillen te achterhalen wordt dan ook sterk aangeraden vervolgonderzoek uit te voeren.

Summary

Within the financial service providers, sensitive customer information is frequently stored, transferred and collected. While information security is generally focused on protecting the confidentiality, integrity and availability of information, information security awareness is also about creating and maintaining security behaviour as a critical element in an effective information security environment. Literature research has shown that despite the use of several controls, organisations continue to experience security breaches. In addition, there are deficiencies in awareness behaviour and security awareness, today the employees are the biggest challenge. A study of ISA within three major banks showed that differentiation in groups was used because of the different risks and employee behaviour, the content of this differentiation was not investigated.

To add new knowledge to the existing knowledge, the following main question would be investigated: "What effect does a differentiation in ISA have on the information security of main branch and branch offices?" To find out this answer, we start with a literature study followed by empirical research. Through six sub-questions, this research will go into important aspects of ISA, which factors about ISA play an important role within the sector, the differences of ISA between head office and branch office employees, which factors influence information security behaviour, which awareness campaigns could possibly contribute to ISA and finally answers the question whether an ISA programme is influenced by the differences between head office and branch office employees. The theoretical part deals with the existing literature, the empirical part of the study deals with the validation of this literature. The validation and actual implementation of the research is done by means of a case study, single embedded design carried out within one of the three major banks in the Netherlands. The case consists of several elements as it investigates the difference between the employees of a branch office and the head office. The research method is shaped by a survey based on the HAIS-Q and is used within the head office and several branches. It takes into account an earlier survey within bank X, also conducted on the subject of ISA.

In total, 87 of 468 employees have filled in the survey, of which 60 complete and 27 incomplete. The results show interesting significant differences between employees of a local branch and employees of the head office. For the focus area Password Management we see the following significant differences: "It's safe to use the same password for social media and work accounts": head office employees (on the KAB dimension Attitude) score higher than branch office employees. In addition, the test shows that branch office employees (on the KAB Attitude dimension) score higher than head office employees on the following item: "It's a bad idea to share my work passwords, even if a colleague asks for it". For the focus area Social Media use, we see the following significant difference: "It's risky to post certain information about my work on social media": head office employees (on the KAB dimension Attitude) score higher than branch office employees.

An important finding in this study concerns an equal ISA level between the two groups of employees. Furthermore, the theory is confirmed by the results showing that head office employees have a higher ISA level for the password management focus area than branch office employees. It is remarkable that the significant differences were not found on the same items in previous research. In addition, no significant differences were found in the area of e-mail use, a limitation from previous research was that there was no situational into the extent to which the respondents had contact with unknown senders. Furthermore, the assumption was made that branch office employees have more contact with unknown senders. Our results show that 17 of 45 head office employees have contact with unknown senders compared to 28 branch office employees. The focus area social media shows an equal level of ISA between the different groups, however, a significant difference was found on a different item than the items on social media in previous research. Based on this item, it can be concluded that the employees of a branch office consider it less risky to post certain information about work on social media.

With the new insights, it can be concluded that the differences between the groups of employees within large bank X are smaller than was initially thought. This conclusion is purely based on the results of the statistical tests, which revealed less significant differences at item level. However, a sample of 60 respondents is too low to be able to make a statement about the entire population. To find out the exact cause of these differences, follow-up research is highly recommended.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Financiële instellingen zijn de laatste jaren steeds vaker het doelwit geworden van cyberaanvallen. Om de cyberaanvallen ofwel IT risico's te voorkomen beschikt De Nederlandsche Bank over adequate procedures en maatregelen. Een van de beheersmaatregelen betreft de bewustwording over informatiebeveiliging in het algemeen en cybersecurity in het bijzonder bij directie, bestuur, medewerkers en verantwoordelijke IT-beveiligingsexperts. Dit betreft onder meer Information Security Awareness (ISA): de mate waarin medewerkers in staat zijn om informatie-incidenten te voorkomen en af te wenden. Daarbij is het bewustzijn en verantwoordelijkheidsgevoel dat de medewerkers hebben bij informatiebeveiliging van groot belang.

1.2. Gebiedsverkenning

Het Information Security Forum (ISF, 2002) definieert Information Security Awareness als de mate waarin elke medewerker het belang van informatiebeveiliging begrijpt, de niveaus van informatiebeveiliging die geschikt zijn voor de organisatie, hun individuele beveiligingsverantwoordelijkheden en handelt hiernaar. Er zijn echter meerdere definities voor Information Security Awareness; *security awareness*, *cyber awareness*, *information awareness, beveiligingsbewustzijn.* In dit onderzoek kunnen deze termen worden gebruikt met de constatering dat deze altijd dezelfde betekenis en definitie hebben zoals eerder genoemd.
Naast technologie wordt menselijk gedrag over het algemeen gezien als de grootste bedreiging voor Information Security (IS) (Baskerville , et al., 2013). Gebruikers veroorzaken regelmatig IS-incidenten door vrijwillig of niet-vrijwillig risicogedrag, zoals onzorgvuldige informatieverwerking, surfen op onbeveiligde webpagina's, nalatig gebruik van mobiele apparaten etc.
Financiële instellingen hebben zich gerealiseerd dat professioneel beheer van IS cruciaal is om de risico's te mitigeren (Hsu, Backhouse, & Silva, 2013). Daarnaast is meting en kwantificering van operationeel risico, dat bestaat uit risico's als gevolg van processen, mensen en systemen, verplicht sinds de internationale bank regelgeving Basel II in 2004. Financiële instelling en financieel dienstverlener heeft in dit onderzoek dezelfde definitie als "*bank*".

1.3. Probleemstelling

Ondanks het gebruik van meerdere controles blijven organisaties beveiligingslekken ervaren. Op basis van door instellingen gemelde incidenten in 2018 ziet DNB als top drie: DDoS-aanvallen, gevolgd door ongeautoriseerde toegang en (on)bewuste 'datalekken'. Recente inzichten hebben geleerd dat aandacht nodig blijft voor het detecteren en analyseren van cyberaanvallen en dat meer aandacht uit zou moeten gaan naar het reageren hierop en het herstel daarna (DNB, 2018). Daarnaast blijkt uit een onderzoek onder 3.000 bedrijfsleiders dat 38% comfortabel is met de toereikendheid van hun medewerkers voor cyberbeveiliging en privacy. Slechts een derde van de ondervraagde vindt dat hun organisatiestructuur en medewerkers volledig klaar zijn om te voldoen aan recente en aankomende vereisten voor cyberbeveiliging, informatiebeveiliging en gegevensgebruik beheer (PwC, 2018).

Terwijl informatiebeveiliging in het algemeen gericht is op het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, gaat het bewust omgaan met informatiebeveiliging om het creëren en behouden van beveiligingsgedrag als kritisch element in een effectieve

informatiebeveiligingsomgeving. Het gedrag van medewerkers speelt een cruciale rol in de effectieve informatiebeveiligingsomgeving (Furnell, Sohrabi Safa , & Von Solms , 2016).

Uit een onderzoek naar ISA binnen 3 grootbanken blijkt dat er differentiatie in groepen is gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers. Over het algemeen zijn de medewerkers op een hoofdkantoor gefocust op het algemene beheer van een bank zonder klantcontact, denk aan compliance, projectmanagement en IT. De medewerkers op een bijkantoor hebben wel direct klantencontact. Deze onderscheidende profielen hebben sterke implicaties voor het beveiligingsgedrag. Uit ditzelfde onderzoek blijkt dat aanvullend onderzoek noodzakelijk is (Bauer & Bernroider, From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization, 2017).

Daarnaast blijkt uit een recent onderzoek uitgevoerd door De Nederlandsche Bank dat 4 op de 10 bijkantoren in de financiële dienstverlening de wet en regelgeving niet naleven. Dit onderzoek heeft plaatsgevonden binnen organisaties waarbij het hoofdkantoor het beleid opstelt en een centrale rol heeft (DNB, 2018). Of dit effect te maken heeft met het bewustwordingsgedrag van de medewerkers van een bijkantoor is onvoldoende onderzocht.

1.4. Opdrachtformulering

Onlangs werd de relatie gemeten tussen de verschillen van individuen en ISA (Butavicius, et al., 2017). Hieruit blijkt dat er aantal verschillen zijn gevonden tussen geslacht, leeftijd, persoonlijkheid en neiging tot het nemen van risico's, en de mate waarin ze variantie in individuele ISA verklaren. In dit onderzoek is gefocust op de 5 persoonlijkheidsfactoren. Het vijf-factorenmodel van persoonlijkheid, wordt beschouwd als het leidende theoretische model voor persoonlijkheid meten en begrijpen. Het bestaat uit de volgende vijf factoren: neuroticisme, extraversie, openheid, gemoedelijkheid en nauwkeurigheid (Costa & McCrae , 1992).
Gezien de beperkte reikwijdte in dit onderzoek dienen er ook andere individuele variabelen worden onderzocht. Zo kan er gekeken worden of het vertrouwen van medewerkers in de technologie een verband heeft met ISA. Dit verschil in combinatie met differentiatie tussen het gedrag van medewerkers op het hoofdkantoor en het gedrag van medewerkers op een bijkantoor. De uitkomsten uit dit aanvullende onderzoek moeten uiteindelijk antwoord geven op de volgende hoofdvraag:

Wat heeft een differentiatie op ISA voor effect op de informatiebeveiliging van hoofd- en bijkantoor?

De hoofdvraag wordt ondersteund door de volgende deelvragen:

1. Wat wordt er onder Information Security Awareness (ISA) verstaan?
2. Wat zijn belangrijke onderdelen van ISA?
3. Welke factoren omtrent ISA spelen een rol binnen de financiële dienstverlening?
4. Wat zijn de verschillen van ISA tussen medewerkers van het hoofdkantoor en bijkantoor?
5. Welke factoren zijn van invloed op informatiebeveiligingsgedrag?
6. Welke bewustmakingscampagnes veranderen informatiebeveiligingsgedrag?

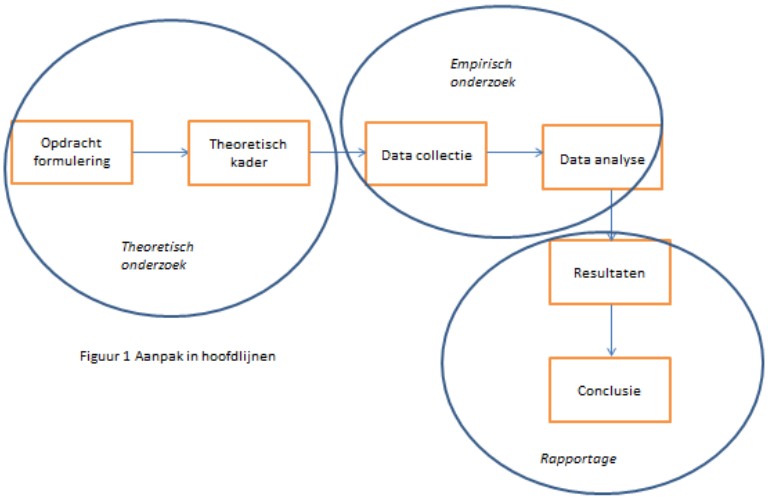
Om een volledig beeld te krijgen van de verschillende definities en begrippen over Security Awareness Information wordt er gestart met een literatuuronderzoek. Om vervolgens de kennis toe te passen binnen de sector financiële dienstverlening is het van belang om de diverse factoren te achterhalen. Essentieel hierbij betreffen de verschillen tussen het hoofdkantoor en bijkantoor. Antwoord op de vraag welke factoren er in algemene zin invloed hebben op beveiligingsgedrag en welke bewustmakingscampagnes informatiebeveiligingsgedrag veranderen zal bijdragen aan het uiteindelijke resultaat van het onderzoek.

1.5. Motivatie / relevantie

De maatschappij wordt dagelijks bedreigd door cyberaanvallen uitgevoerd door verschillende partijen. Gezien de toename van digitalisering zal de urgentie van de bestrijding tegen cyberaanvallen belangrijker dan ooit zijn. Veiligheid hangt af van de prikkels van bedrijven, burgers en regeringen. Deze actoren kunnen een sterkere verdediging aannemen, aanvallen afzwakken of negeren, privacy verbeteren of ondermijnen (Schoof, 2018).
In diverse wetenschappelijke onderzoeken wordt aangegeven dat er tot op heden nog te weinig onderzoek is gedaan naar diverse relaties en bewustwording van informatiebeveiliging. Zo geeft een onderzoek naar het effect op compliance kennis en bewustwording aan dat de resultaten vanuit het onderzoek pas generaliseerbaar zijn indien de bevindingen binnen andere bedrijven en andere industrieën worden getoetst . (Kim & Kim , 2017). In dit onderzoek wordt nu getoetst wat het effect is op bewustzijn van informatiebeveiliging binnen de financiële dienstverlening zodat nieuwe kennis kan worden toegevoegd aan de bestaande wetenschap.

1.6. Aanpak in hoofdlijnen

Na formulering van de probleemstelling zijn de hoofdvragen en deelvragen opgemaakt. De probleemstelling wordt gevolgd door het theoretische kader waarin de onderzoeksaanpak wordt toegelicht en de literatuurstudie wordt uitgevoerd. Met de resultaten uit het literatuuronderzoek kan een vervolg worden gegeven aan het tweede deel van het onderzoek namelijk het empirische deel. Het empirische deel start met het hoofdstuk over de methodologie met de focus op het conceptuele en technische ontwerp en eindigt in reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten. Uiteindelijk wordt het onderzoek afgerond met een weergave van de resultaten, discussie en conclusie gevolgd door aanbevelingen voor de praktijk en verder onderzoek.



Figuur 1 Aanpak in hoofdlijnen

2. Theoretisch kader

2.1. Onderzoeksaanpak

Om de uitvoering van het literatuuronderzoek een richting te geven wordt er gebruik gemaakt van de literatuurstudie van Saunders (Lewis, Saunders, & Thornhill, 2019). In hoofdstuk 1 is de wetenschappelijk relevante probleemstelling inclusief hoofd- en deelvragen geformuleerd. Om antwoord te kunnen geven op de hoofd- en deelvragen wordt er in dit hoofdstuk een onderzoeksstrategie ontworpen. Er wordt gestart met het zoeken van bestaande kennis over de probleemstelling middels een literatuuronderzoek. Het literatuuronderzoek vormt een belangrijke verbinding tussen de probleemstelling en de te verzamelen gegevens, deze volgt in hoofdstuk 3. Om de validiteit en betrouwbaarheid van het onderzoek te verhogen is er gebruikgemaakt van wetenschappelijke publicaties. De bronnen zijn middels de zoekmachine van Google Scholar en de universiteitsbibliotheek van de Open Universiteit geraadpleegd. De ingestelde queries en bronnen worden expliciet aangegeven in hoofdstuk 2.2. Uitvoering.

2.2. Uitvoering

Om een beeld te geven over de uitvoering van het literatuuronderzoek wordt er in de volgende stappen uitleg gegeven.

Stap 1

Er is gestart met het definiëren van diverse zoektermen, definities en synoniemen. Dit heeft geresulteerd in een hoeveelheid literatuur. Om de maatschappelijke relevantie te onderzoeken is tevens gebruikgemaakt van grootschalige onderzoeken uitgevoerd door overheidsinstellingen of grote relevante organisaties binnen de betreffende branche. De artikelen in de gevonden literatuur zijn beoordeeld op bruikbaarheid. Dit heeft plaatsgevonden door de samenvatting en conclusie door te lezen, het artikel globaal door te nemen en de synoniemen en definities op te zoeken middels de zoekfunctie “F5” in het betreffende artikel. De uitgebreide versie van de vereisten waar de artikelen aan moeten voldoen conform de theorie zijn opgenomen in bijlage 1 (Bell, Maidenhead).

Stap 2

In de zoekmachine van Google Scholar en de Universiteitsbibliotheek hebben verschillende zoektermen hits gekregen. Er zijn diverse combinaties gebuikt om rekening te houden met representativiteit. Vervolgens zijn de hits geselecteerd op bruikbaarheid. In de situaties waarin een artikel niet via Google Scholar leesbaar was maar wel via de Universiteitsbibliotheek is dit artikel toegevoegd aan “Relevant en/of gebruikt” in de tabel van Universiteitsbibliotheek. Bij “bekeken” wordt de hoeveelheid bekeken artikelen weergegeven, dit zijn de artikelen die een korte analyse hebben gehad. Google Scholar heeft een extra filter met “resultaten sinds 2016” deze filter is toegevoegd om de representativiteit te waarborgen. De Universiteitsbibliotheek heeft de volgende extra filter “Peer reviewed”, deze filter is toegevoegd om de kwaliteit van de resultaten te waarborgen. Hieronder wordt een korte weergave gegeven van het aantal hits, de hoeveelheid hits die bekeken zijn, welke hits relevant waren en welke literatuur uiteindelijk is gebruikt in het onderzoek.

Stap 3

In de derde stap zijn de relevante artikelen verder onderzocht middels de sneeuwbalmethode. Via de deze methode zijn de literatuurlijsten van de relevante artikelen gebruikt om tot nieuwe bruikbare artikelen te komen. De lijst samengesteld vanuit stap 1 en 2 vormt hiervoor de basis. Er is gekozen voor de “Forward snowballing” methodiek. Deze methodiek verwijst naar het identificeren van nieuwe artikelen op basis van de bronnen die in deze betreffende artikelen worden aangehaald. In de tabellen zijn de artikelen opgenomen die hiervoor zijn gebruikt. Er wordt eerst naar de titel van

het artikel gekeken, vervolgens naar de samenvatting, de plaats van de citering in het artikel en vervolgens naar het hele artikel. Na het toepassen van de “Forward snowballing” methodiek zijn er geen nieuwe bruikbare artikelen vastgesteld.

Tabel 1: Zoekacties in Google Scholar

Zoektermen Google scholar	Resultaten	Resultaten sinds 2016	Bekeken	Relevant	Gebruikt
Information Security Awareness	3.350.000	228.000	31	16	8
Security awareness	3.320.000	234.000	24	8	4
Cyber awareness	452.000	78.200	10	6	2
Information awareness	4.420.000	1.070.000	19	3	1
Information security awareness banking	502.000	47.700	16	9	5
Branch and main offices employees attitudes	207.000	26.500	10	3	2
Security awareness influence	2.180.000	179.000	12	8	6
Informatiebeveiliging	1.010	166	9	4	0
Bewustwording gedrag	13.600	2.340	18	5	1
Beveiliging gedrag	10.200	1.120	4	0	0
Awareness campaigns change information security behavior	241.000	38.800	22	15	5
Information Security Awareness individuals	1.970.000	109.000	18	8	4

Tabel 2: Zoekacties in de Universiteitsbibliotheek

Zoektermen Universiteitsbibliotheek	Resultaten	Peer reviewed	Bekeken	Relevant	Gebruikt
Information Security Awareness	419.661	178.215	28	17	7
Security awareness	501.110	198.124	31	13	8
Cyber awareness	43.007	15.866	19	8	1
Information awareness	1.815.472	1.061.320	35	18	5
Security awareness influence	1.815.472	120.971	16	9	3
Information security awareness banking	42.580	13.867	19	6	1
Awareness campaigns change information security behavior	43.118	22.944	11	2	2
Information Security Awareness individuals	273.489	149.243	9	2	2

2.3. Resultaten en conclusies

Hierbij volgen de antwoorden op de onderzoeksvragen op basis van de gevonden literatuur. Deze eindigen in een conclusie van het theoretisch kader.

2.3.1. Wat wordt er onder Information Security Awareness (ISA) verstaan?

Recente onderzoeken naar informatiebeveiliging hebben aangetoond dat er tekortkomingen zijn in menselijk gedrag en beveiligingsbewustzijn de grootste uitdaging betreft. Information security awareness (ISA) speelt een cruciale rol bij het beschermen van informatiebeveiliging (Marks & Rezgui, 2015). Binnen de ISA literatuur wordt het begrip bewustzijn bijvoorbeeld gedefinieerd als "technologie bewustzijn” ofwel “Door de gebruiker verhoogd bewustzijn van en interesse in kennis over technologische problemen en strategieën” (Dinev & Hu, 2007). Veel organisaties erkennen dat hun werknemers worden beschouwd als de zwakste schakel in informatiebeveiliging, het is dan ook van belang om risico’s in kaart te brengen in verband met de bewustwording van informatiebeveiliging.

ISA wordt algemeen erkend door veel onderzoekers, er zijn verschillende definities en percepties van ISA beschreven in de literatuur. De verschillen in de definities kunnen in meerdere componenten worden gedeeld. Zo spreken Aggeliki Tsohou, Siponen en Hyeun-suk Rhee over bewustzijn en waakzaamheid van verschillende informatiebeveiliging bedreigingen en het waarnemen van een kwetsbaarheid (Karyda, Kiountouzis, Kokolakis , & Tsohou, 2015) (Siponen, 2000) (Cheong-Tag , Hyeun-Suk, & Young, 2005). Burcu Bulgurcu heeft het over de algemene kennis over informatiebeveiliging van een werknemer en zijn kennis van de Information Security Policy (ISP) van zijn organisatie (Cavusoglu, Benbasat, & Bulgurcu, Roles of Information Security Awareness and Perceived Fairness in Information Security Compliance, 2009) (Cavusoglu, Benbasat, & Bulgurcu, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and

Information Security Awareness, 2010). De verschillende componenten staan met elkaar in verband en worden niet los van elkaar gezien. In dit onderzoek wordt ISA dan ook gedefinieerd als “het bezitten van voldoende kennis en het bewustzijn zijn van informatiebeveiliging”.

Binnen de financiële dienstverlening wordt veelvoudig gevoelige klantinformatie opgeslagen, overgedragen en verzameld. Naast eerdere constateringen over de hoeveelheid toenemende cyberaanvallen is het dus ook essentieel dat de medewerkers zich bewustzijn van informatiebeveiliging voor de bescherming van gevoelige gegevens van klanten. Ook dit is een vorm van information security awareness (Mani, Mubarak , & Choo, 2014).
Veel onderzoekers hebben bewustmaking resultaten voor informatiebeveiliging onderzocht, echter is de hoeveelheid gebruikte methodes en modellen waarmee ISA is onderzocht enorm. Hierbij zijn de onderdelen niet alleen beperkt tot individueel niveau, maar ook tot organisatorisch en technisch niveau binnen een organisatie. Hier wordt verder ingegaan bij 2.3.2.

2.3.2. Wat zijn belangrijke onderdelen van ISA?

In het vorige deel zijn meerdere definities en uitleg over ISA gegeven. Het verhogen van ISA binnen een organisatie kent verschillende benaderingen. Over het algemeen spreekt men in de literatuur over het verbeteren van individueel beveiligingsgedrag en het aanpassen van de cultuur binnen de organisatie. Bewustmaking en veranderend beveiligingsgedrag kunnen een uitdaging zijn, medewerkers moeten betrokken zijn bij de realiteit van bedreigingen en dienen het proces te begrijpen om problemen of zorgen te identificeren en aan te pakken. Ofwel medewerkers moeten gemotiveerd worden om positief gedrag toe te passen en risicopercepties te veranderen (Fischer, Grau, & Roper, 2006). Het verhogen van information security awareness kent diverse benaderingsthema’s of onderdelen binnen de literatuur, er volgt een korte weergave over deze verschillende onderdelen.

Organisatorisch perspectief

In de literatuur zijn diverse invalshoeken en kenmerken over ISA te vinden, een aantal van deze resultaten hebben een breder perspectief waarbij er niet alleen gefocust wordt op het individuele gedrag van een medewerker. Zo wordt uit een van de onderzoeken geconcludeerd dat impliciete veranderingen niet alleen beperkt worden tot individueel niveau, maar ook uitgebreid moeten worden naar het organisatorische en technische niveau. Factoren worden ingedeeld onder de vier thema's: organisatorisch, technologisch, politiek en sociaal. Zo is uit empirisch onderzoek gebleken dat betrokkenheid van het topmanagement, middelen en rendement van investeringen belangrijke bewustmaking initiatieven op het gebied van informatiebeveiliging betreft (El-Haddadeh, Karyda, & Tsohou , 2012). In een andere studie worden de invalshoeken van socialisatie, externalisatie, internalisatie en combinatie (SECI model) gebruikt om ISA te meten. Er is ontdekt dat socialisatie, internalisatie en combinatie positieve invloed heeft op het ontwikkelen van een cultuur van informatiebeveiliging en het vergroten van het bewustzijn van informatiebeveiliging bij medewerkers (Mani, Mubarak , & Choo, 2014).

Individueel perspectief

In andere literatuuronderzoeken wordt wel specifiek ingegaan op individueel perspectief, zo wordt er gekeken naar de drijfveren achter het betreffende gedrag en belichten ze welke interventies het meest effectief kunnen worden gebruikt om het betreffende gedrag te beïnvloeden. Zo blijkt uit een onderzoek dat TRA individuele intenties zijn om een gedrag uit te voeren. Neutralisatietechnieken worden weerspiegelt om zich aan te trekken of geen gedrag te vertonen, hier specifiek gerelateerd aan niet-conform gedrag inzake informatiebeveiliging. Zo blijkt uit de resultaten van dit onderzoek dat verbeteringen van attitudes en persoonlijke en sociale normen samenhangen met een verhoogde intentie voor compliant informatiebeveiligingsgedrag (Bauer & Bernroider, From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization, 2017).

In recente onderzoeken (vanaf 2014) naar individueel perspectief wordt vaker gebruikt gemaakt van "Human Aspects of Information Security Questionnaire" (HAIS-Q). HAIS-Q wordt ingezet om de effectiviteit van verschillende informatietechnologie (IT) controlestrategieën te evalueren, of om de beveiligingsstatus van een organisatie te volgen. Er wordt gefocust op drie kernelementen; kennis, houding en gedrag van medewerkers. Daarnaast worden de kernelementen gecombineerd met zeven focusgebieden in informatiebeveiliging; wachtwoordbeheer, e-mailgebruik, internetgebruik, gebruik van sociale media, mobiele apparaten, informatieverwerking en incidentrapportage (Butavicius, Jerram , McCormac , Parsons , & Pattinson , 2014). Zo is onlangs geconstateerd dat consciëntieusheid, aanvaardbaarheid, emotionele stabiliteit en het nemen van risico's de variantie in de ISA van individuen significant verklaarden, terwijl leeftijd en geslacht dat niet deden. Vanwege de recente ontwikkelingen moet hierbij wel de kanttekening worden gemaakt dat de noodzaak aanwezig is om toekomstig onderzoek om individuele verschillen en hun impact op ISA verder te onderzoeken (Butavicius, et al., 2017). Daarnaast is de HAIS-Q methodiek op sommige vraagstukken verouderd en zijn er mogelijkheden om in toekomstig onderzoek HAIS-Q in een actuele vorm toe te passen.

2.3.3. Welke factoren omtrent ISA spelen een rol binnen de financiële dienstverlening?

Zoals eerder onderzocht is professioneel management van information security van groot belang binnen banken (Hsu, Backhouse, & Silva, 2013). Sinds een aantal jaar is men begonnen met het uitvoeren van preventieve controles in de vorm van Information Security Policies (ISP). ISP is een beleid waarin verplichte organisatorische regels, richtlijnen en vereisten zijn vastgelegd. De ISP is daarom ook een belangrijke controle voor het ondersteunen van informatiebeveiliging. Uit onderzoek blijkt dat zelfs het bestaan ervan een positief effect heeft op de het bewustzijn gedrag van medewerkers (Angermeier, Boss, Boss, Kirsch, & Shingler, 2009). ISP heeft drie neutralisatietechnieken; ontkenning van schade, beroep op hogere loyaliteit en verdediging van noodzaak. Resultaten laten zien dat deze technieken belangrijk zijn binnen de financiële dienstverlening, er wordt aangeraden om dit verder te onderzoeken (Bauer, Bernroider, & Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, 2017).

ISA binnen de financiële dienstverlening is vergeleken met andere verschillende industrieën zoals Healthcare, Higher Education en Retail (Goel, Kam, & Mattson , 2019). Een kenmerkende factor binnen de financiële dienstverlening is formeel toezicht, zo moeten banken voldoen aan een reeks voorschriften zoals bijvoorbeeld Sarbanes-Oxley Act (SOX). Vanuit het oogpunt van informatiebeveiliging vereisen deze voorschriften dat financiële instellingen administratieve, technische en fysieke beveiligingen om de vertrouwelijkheid, integriteit en beschikbaarheid van klantinformatie te beschermen. Als gevolg hiervan heeft men aanzienlijke inspanningen geleverd om zich te ontwikkelen op algemene ISA en trainingsprogramma's (Dinev & Hu, 2007). Echter kan het niet naleven van deze informele spelregels net zo schadelijk zijn, zo kan de organisatie op deze manier normatieve legitimiteit verliezen in een bepaalde marktruimte, wat kan leiden tot verlies van reputatie, prijssterkte en klanten (Scott, 2008).

Juist door de schade die een ineffectief ISA programma met zich meebrengt is het van belang dat er systematisch geplande interventies zijn om beveiligingsinformatie te waarborgen. Uit een onderzoek naar de ISA programma's binnen 3 grootbanken blijkt dat IS-managers meer aandacht moeten besteden aan een cyclisch managementproces, zoals bijvoorbeeld het ISA programma evalueren op basis van de PDCA-cyclus. Daarnaast werd aangetoond dat een interactieve benadering het meest gunstig lijkt voor het vergroten van de perceptie door bankmedewerkers van IS-risico's (Bauer, Bernroider, & Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, 2017). In dit onderzoek wordt tevens aangegeven dat er verder onderzoek moet worden uitgevoerd

naar welke soorten persoonlijkheden meer gevoelig zijn voor bepaalde ISA-interventies of ISA-programmabenaderingen. Daarnaast blijkt een verschil van naleving van ISA programma's tussen hoofdkantoor en bijkantoor, echter wordt ook aanbevolen om dit onderzoek uit te breiden.

Als we de kenmerkende factoren van medewerkers binnen de financiële dienstverlening onderzoeken zien we in de huidige literatuur een aantal constateringen. Zo blijkt uit een kwalitatief onderzoek naar de ervaringen met IS van bankmedewerkers dat het beperken van IS-risico's werd gezien als een gedeelde verantwoordelijkheid tussen de medewerker en de bredere bankbeveiliging systemen. De opvattingen van het personeel over beveiligingsinbreuken hing samen met het daaropvolgend verlies van vertrouwen in de bank door het publiek en werd gezien als een belangrijk en centraal thema voor medewerkers (Berkovsky, et al., 2017). In een ander onderzoek is middels HAIS-Q de verschillen van ISA-niveaus van bankmedewerkers en algemene werknemers uit overige organisaties vergeleken. Er werd aangetoond dat het gemiddelde niveau van ISA voor bankmedewerkers ongeveer 20% hoger ligt dan voor de algemene medewerkers uit overige organisaties (Butavicius, et al., 2016). Echter vonden beide onderzoeken plaats binnen grote banken in Australië en Nieuw-Zeeland, het kan zijn dat de culturele verschillen deze bevindingen kunnen beïnvloeden waardoor aanvullend onderzoek noodzakelijk wordt geacht.

Kortom, door een tekort aan recente onderzoeken naar ISA binnen de financiële dienstverlening in algemene zin, de verschillen in naleving tussen hoofdkantoor en bijkantoor én de gevonden resultaten die onvoldoende zijn om te generaliseren is er voldoende belang bij toekomstig onderzoek op deze onderwerpen. Dit leidt tot de volgende hypothese:

H1: Medewerkers van een hoofdkantoor volgen de ISA programma's beter op dan de medewerkers van een bijkantoor.

2.3.4. Wat zijn de verschillen van ISA tussen medewerkers van het hoofdkantoor en bijkantoor?

Uit de analyse van voorgaande literatuurstukken blijkt veelvoudig dat er meer empirisch bewijs nodig is op gedragstheorieën om de aanhoudende verschijnselen van niet-naleving van ISP door werknemers verder te onderzoeken, in het bijzonder in hoge mate bij gevoelige financiële instellingen. Daarnaast blijkt er een verschil van naleving van ISA programma's tussen hoofdkantoor en bijkantoor. Banken dienen hun ISA programma's aan te passen door onderscheid te maken tussen de IS behoeften van gebruikersgroepen, in termen van hoofdkantoor- en bijkantoor (Bauer, Bernroider, & Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, 2017). Uit dit onderzoek blijkt tevens dat de differentiatie in groepen is gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers. Over het algemeen zijn de medewerkers op een hoofdkantoor gefocust op het algemene beheer van een bank zonder klantcontact, denk aan compliance, projectmanagement en IT. De medewerkers op een bijkantoor hebben wel direct klantencontact. Deze onderscheidende profielen hebben sterke implicaties voor het beveiligingsgedrag van IS, dat moet worden beïnvloed door ISA-programma's ontworpen en uitgevoerd door IS-managers.

Om bovengenoemde verschillen te benadrukken is er gebruikgemaakt van andere theorieën. Rond 1978 merkte Rousseau al op dat zowel individuele verschillen als kenmerken van organisatorische instellingen van cruciaal belang voor alle fasen van organisatieonderzoek (Rousseau, 1978). In een onderzoek naar verschillen in gedrag tussen medewerkers van filiaalbanken en hoofdkantoorbanken wordt geconcludeerd dat de medewerkers van filiaalbanken een lagere betrokkenheid tonen dan de medewerkers van het hoofdkantoor (Clinebell & Sharon , 2005). Of er een verband is met ISA wordt niet genoemd evenals de reden waarom de medewerkers een lage betrokkenheid laten zien. Wel lijkt betrokkenheid van medewerkers een belangrijk bemiddelingseffect, onderzoek omtrent dit

onderwerp moet nieuwe inzichten geven. Hoe wordt betrokkenheid bereikt door ISA-interventies, wat op zijn beurt de naleving van gedrags-ISP moet bevorderen.

Mede wegens de beperkte hoeveelheid onderzoeken naar ISA van bankmedewerkers is er onlangs een onderzoek uitgevoerd binnen een van de grootste banken van Nederland. Binnen dit onderzoek is tevens een differentiatie gemaakt tussen medewerkers van het hoofdkantoor en de medewerkers van een bijkantoor. Om deze verschillen in kaart te brengen, is er gebruik gemaakt van een aangepaste versie van de HAIS-Q vragenlijst waarin de volgende aandachtsgebieden zijn opgenomen: Wachtwoordbeheer, gebruik van e-mail, gebruik van sociale media, mobiele apparaten en rapportage van incidenten. Deze aandachtsgebieden zijn uitspraken op basis van het kennis-, attitude- en gedragsmodel. Dit empirische onderzoek heeft de volgende bevindingen opgeleverd: Binnen de 'mobiele apparaten' en 'incident reporting' focusgebieden konden geen significante verschillen worden gevonden. Echter, binnen de overige drie gebieden, werden verschillende significante verschillen tussen beide groepen ontdekt (Takens, 2020). Er is o.a. geconcludeerd dat medewerkers van het hoofdkantoor meer bewust zijn van het gebruik van sociale media. Beide groepen verschillen niet van elkaar als het gaat om kennis van het beleid op het gebied van sociale media privacy instellingen. De medewerkers van het hoofdkantoor laten echter een betere houding zien. Om de bevindingen te valideren en hiermee de betrouwbaarheid van het onderzoek te verhogen is het raadzaam om de resultaten op de volgende onderwerpen, binnen deze bank nogmaals te toetsen:

Wachtwoordbeheer
Uit de resultaten is gebleken dat medewerkers van het hoofdkantoor een betere houding (A) aannemen ten aanzien van het gebruik van sterke wachtwoorden. Tegelijkertijd is er geen verschillen waargenomen in de gerelateerde kennis- en gedragsverklaringen. In het onderzoek wordt sterk aangeraden om verder te onderzoeken hoe de medewerkers van een bijkantoor overtuigd kunnen worden van de voordelen van het gebruik van sterke wachtwoorden. Hierdoor wordt de volgende hypothese getoetst:

H2: De houding van medewerkers van een bijkantoor ten opzichte van het gebruik van sterke wachtwoorden is waarschijnlijk lager dan die van de medewerkers van het hoofdkantoor.

E-mail
Er zijn interessante bevindingen geconstateerd die gerelateerd zijn aan e-mails van onbekende afzenders. Medewerkers van een bijkantoor hebben een aanzienlijk betere kennis van het beleid en de procedures met betrekking tot klikken op links en het openen van bijlagen. Ondanks deze betere kennis laten zij dit niet zien in hun gedrag. Een beperking in dit onderzoek is dat men meerdere veronderstellingen niet heeft kunnen valideren, omdat men zich niet bewust was van de mate waarin de respondenten e-mailcontact hebben met onbekende partijen. Bij het onderzoeken van de volgende drie hypothesen wordt aangeraden om speciale aandacht te besteden aan de mate waarin beide groepen e-mailcontact hebben met onbekende afzenders.

H3.1: De kennis van de medewerkers op een bijkantoor over de behandeling van e-mails van onbekende afzenders is waarschijnlijk hoger dan die van de werknemers op het hoofdkantoor.

H3.2: Medewerkers van een bijkantoor die kennis hebben van het aanklikken van links in e-mails van onbekende afzenders, zullen deze kennis waarschijnlijk niet in de praktijk brengen.

H3.3: Het is onwaarschijnlijk dat medewerkers van het hoofdkantoor kennis nodig hebben van het aanklikken van links in e-mails van onbekende afzenders om het gedrag te kunnen toetsen.

In 2.3.3 werd kort stilgestaan op het kernmerk “formeel toezicht”. Nationaal gezien is De Nederlandsche Bank (DNB) de centrale bank van Nederland. De DNB houdt toezicht op de banken in Nederland, bewaakt de financiële stabiliteit en adviseert de regering. Uit nationale wetgeving blijkt verschil tussen een dochteronderneming en een bijkantoor, zo is een dochteronderneming een aparte juridische entiteit. Elke financiële instelling met een vergunning uit een EER-lidstaat kan een bijkantoor openen. Hier is geen aparte vergunning voor nodig waardoor het toezicht vanuit de toezichthouder (hoofdkantoor) verschilt. Het toezicht vanuit het hoofdkantoor op de bijkantoren is een probleem blijkt in een rapport van de algemene rekenkamer. Zo wordt als voorbeeld genoemd dat informatie uitwisseling tussen hoofdkantoor en bijkantoor te wensen over laat (Rekenkamer, 2009). In toekomstig onderzoek is het van belang om te achterhalen of er een verband is met het bewustwordingsgedrag van medewerkers en het verschil van medewerkers tussen hoofd en bijkantoor.

2.3.5. Welke factoren zijn van invloed op informatiebeveiligingsgedrag?

Om bewustwordingsgedrag van medewerkers of individuen beter te begrijpen worden diverse theorieën in de literatuur onderzocht. Met name het achterhalen van de factoren die van invloed zijn kan helpen bij het vormgeven van nader onderzoek. Zo wordt er conform de theorie van “Planned Behaviour” aangegeven dat gevoelens, gedachten, gedragingen en acties van individuen beïnvloed worden door hun interactie met andere personen. Ofwel: Theory of Reasoned Actie (TRA); het beschrijft de veranderingen in menselijk gedrag gebaseerd op het perspectief van sociale invloed (Ajzen & Fishbein, On construct validity: A critique of Miniard and Cohen's paper, 1981). In een ander onderzoek blijkt dat kennisdeling een positief effect heeft op beveiligingsgedrag van werknemers. De resultaten van de gegevensanalyse lieten daarnaast zien dat het verdienen van een beloning of het verkrijgen van promotie als een extrinsieke motivatie positief effect heeft op beveiligingsgedrag. Echter werden de gegevens verzameld bij verschillende Maleisische organisaties waardoor generalisatie van de bevindingen kunnen worden verhoogd door een grotere steekproefomvang te overwegen (Furnell, Sohrabi Safa , & Von Solms , 2016). Dat verder onderzoek naar de factoren van invloed op beveiligingsgedrag noodzakelijk is, blijkt uit het volgende onderzoek. In hetzelfde jaartal wordt elders geconcludeerd dat verschillende soorten werknemers op verschillende manieren van beloningen reageren. Dit heeft zich namelijk niet vertaald in een toename van de houding van werknemers (Butavicius, et al., 2017).

Leiderschap

Uit meerdere onderzoeken blijkt leiderschap een belangrijke factor die invloed heeft op informatiebeveiligingsgedrag van medewerkers. Managementstudies hebben aangetoond dat leiderschapsstijlen een invloed hebben op de prestaties van werknemers. Het aanmoedigen en monitoren van werknemers in een organisatie is van belang (Kaushal, 2011). Uit een van deze empirische onderzoeken naar leiderschapsstijlen blijkt namelijk dat transectioneel leiderschap een direct en indirect positief effect heeft op het informatiebeveiligingsgedrag en nalevingsgedrag van medewerkers (Balakrishnan & Humaidi , Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness, 2015). Deze bevindingen worden versterkt door het feit dat managers een plicht hebben op het gebied van gezag en leiderschap en het vaststellen van het nalevingsbeleid. Er zijn immers verschillen waargenomen op de manier waarop medewerkers denken over de gestelde regels. Om deze reden moet er aandacht worden gegeven aan de houding van een individu, zijn redeneerpatronen en zelfreflectie (Mudrack, 2007).

Cultuur

In meerdere onderzoeken blijkt de informatiebeveiligingscultuur een belangrijke factor van invloed. Zo blijkt uit het volgende onderzoek dat informatieveiligheidsbewustzijn, gedrag en organisatiecultuur de belangrijkste elementen zijn waarmee rekening moet worden gehouden. Echter is het creëren van een veiligheidscultuur binnen een organisatie een lange termijn

investering. Het vereist constante inspanningen om te groeien en te onderhouden (Clarke, Furnell , & Sherif, 2015). De waarden in verschillende culturen kunnen van elkaar verschillen. Conform onderzoek kan dit worden onderverdeeld in vier factoren (1) Macht (2) Individualisme vs Collectivisme; (3) Mannelijkheid versus vrouwelijkheid en (4) vermijden van onzekerheid. In meer individualistische culturen, zoals het Westen, hebben medewerkers de neiging om zichzelf te definiëren in termen van hun interne kenmerken zoals doelen, voorkeuren en houding (Hofstede, Hofstede, & Minkov, 2005).

Vertrouwen

Wat opvalt is dat er in meerdere onderzoeken het element “vertrouwen” wordt genoemd. Vertrouwen is een van de belangrijke elementen in een digitale omgeving. Ondanks de hoeveelheid elementen is er weinig empirisch onderzoek gedaan naar de relatie tussen ISA en vertrouwen in de technologie. Vertrouwen wordt een complex fenomeen genoemd dat met verschillende afhankelijkheden te maken heeft. Zo is vertrouwen een weerspiegeling van de technologie, sociaal en psychisch. Aan de andere kant kan het vertrouwen deel uitmaken van de persoonlijkheid of worden geassocieerd met een het geloof van het individu in een organisatie die gebaseerd is op de normen, voorschriften, het beleid en de procedures van de organisatie (Davis , Mayer, & Schoorman, 1995). Het belangrijke element vertrouwen in de technologie in combinatie met de hoeveelheid uitgevoerde empirische onderzoeken binnen de financiële dienstverlening maakt op dat het van belang is om nieuwe kennis aan de bestaande kennis toe te voegen. Dit leidt tot de volgende hypothese:

H4: Medewerkers met vertrouwen in de technologie hebben positieve invloed op informatiebeveiligingsgedrag.

2.3.6. Welke bewustmakingscampagnes veranderen informatiebeveiligingsgedrag?

Zoals eerder aangegeven is het kennen van de huidige staat van factoren die van invloed zijn op werknemers belangrijk. Het stelt bedrijven in staat om individuele en op maat gemaakte campagnes voor beveiligingsbewustzijn samen te stellen. Het primaire doel van die campagnes op maat is niet alleen om medewerkers op te leiden, maar ook om hen te overtuigen om een manier van werken te veranderen. Helaas voldoen medewerkers niet altijd aan het opgestelde beleid of het verwachte gedrag. Daar zijn veel mogelijke redenen voor, twee van de meest voorkomende zijn de medewerkers die zich niet bewust zijn (of nemen de risico's niet waar) of kennen/begrijpen de risico’s niet volledig (Balakrishnan & Humaidi , Exploratory Factor Analysis of User’s Compliance Behaviour towards Health, 2013). Volgens een onderzoek van National Institute of Standards and Technology is bewustzijn geen training maar simpelweg de aandacht op beveiliging weerleggen. Bewustmakingscampagnes zijn bedoeld om individuen in staat te stellen IT-beveiligingsproblemen te herkennen en dienovereenkomstig reageren. Het identificeert het feit dat mensen niet alleen op de hoogte moeten zijn van mogelijke cyberrisico's, maar dienen zich hier ook naar te gedragen (Hash & Wilson, 2003). Een model gezien in meerdere casestudies is het Integrated Behavioral Model (IBM). IBM is gebaseerd op het menselijk gedrag wat wordt beïnvloed door vijf factoren: kennis en vaardigheden, extraversie, gewoonte, intentie en omgevingsbeperkingen. Zo wordt er bijvoorbeeld aangegeven dat in plaats van een algemeen doel uit te dragen, zoals het vergroten van de informatiebeveiliging, bewustmakingsacties specifieke houdingen en overtuigingen van werknemers moeten beïnvloeden. Om IBM te gebruiken bij informatiebeveiliging, dient het daarom toegepast te worden op een specifiek gedrag dat voldoet aan informatiebeveiliging (Schütz, 2018).

Het juiste gedrag van medewerkers is soms lastig te meten, immers het juist beantwoorden van vragen betekent niet direct dat een medewerker gemotiveerd is om zich te gedragen volgens de kennis die is opgedaan tijdens een bewustwordingsprogramma. Een campagne moet eenvoudig consistent zijn met gedragsregels die mensen kunnen volgen (Ajzen, Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior., 2002). Gebaseerd op een

onderzoek naar verschillende succesvolle en niet-succesvolle veiligheidsbewustmakingscampagnes is er geconcludeerd dat de volgende factoren nuttig kunnen zijn bij het vergroten van de effectiviteit van huidige en toekomstige campagnes: (1) veiligheidsbewustzijn moet professioneel voorbereid en georganiseerd zijn (2) angst oproepen bij medewerkers is geen effectieve tactiek, het kan medewerkers afschrikken (3) campagnes moeten uitvoerbaar zijn en voorzien zijn van feedback (4) zodra medewerkers bereid zijn tot verandering is opleiding en continue feedback als begeleiding tijdens dit proces noodzakelijk (5) de nadruk op verschillende culturele contexten en kenmerken is nodig bij het opzetten van cyberveiligheidscampagnes (Bada, Nurse, & M. Sasse, 2019).

Om de campagnes te vergelijken binnen de financiële dienstverlening is er gezocht naar literatuur met diverse programma's binnen verschillende banken. Uit een van deze onderzoeken blijkt dat één op drie onderzochte banken een volledig scala van aanbevelingen vanuit de literatuur had overgenomen in haar bewustwordingscampagne. Dit bleek een positieve impact te hebben op de waargenomen IS-risico's, het erkennen van verantwoordelijkheden, en het toekennen van belang aan IS. Bij de overige twee banken bleken minder alomvattende strategieën te zijn geïmplementeerd, hier zijn minder positieve implicaties waargenomen (Bauer, Bernroider, & Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, 2017).

2.4. Doel van het vervolgonderzoek

We weten nu dat ondanks het gebruik van meerdere controles organisaties beveiligingslekken blijven ervaren en dat er tekortkomingen zijn in bewustwordingsgedrag en beveiligingsbewustzijn van medewerkers de grootste uitdaging betreft. Samenvattend wordt ISA gedefinieerd als "het bezitten van voldoende kennis en het bewustzijn zijn van informatiebeveiliging", een verhoging van ISA binnen een organisatie is benodigd om de beveiligingslekken te reduceren. Er zijn meerdere perspectieven zoals individueel of organisatorisch en er zijn meerdere modellen en methodes denk aan TRA en HAIS-Q die ISA kunnen onderzoeken.

Als gevolg van het formele toezicht blijkt dat er binnen de financiële dienstverlening veelvoudig gebruik wordt van ISA campagnes en algemene trainingsprogramma's. Er wordt in de literatuur aanbevolen om eerst de verschillende persoonlijkheden van medewerkers te onderzoeken alvorens bewustwordingsprogramma's uit te zetten. Of deze campagnes ook hebben geleid tot een verhoging van ISA worden wisselende resultaten over gegeven. Dit is tevens sterk afhankelijk van diverse factoren, er wordt dan ook meerdere keren aangegeven dat meer onderzoek naar ISA noodzakelijk is. Wat opvalt is dat er in een aantal onderzoeken binnen financiële instellingen verschillen in gedrag tussen medewerkers van bijkantoren en hoofdkantoorbanken worden gemeten evenals de naleving van ISA programma's. Er lijken een aantal verbanden te zijn echter is dit onvoldoende om de resultaten te generaliseren.

Met de resultaten uit het literatuuronderzoek kan een vervolg worden gegeven aan het tweede deel van het onderzoek namelijk het empirische deel. Het doel van het empirisch onderzoek is om de gevonden resultaten uit de literatuur te toetsen binnen een financiële instelling. Immers tot op de dag van vandaag zijn er nog steeds een groot aantal beveiligingsinbreuken veroorzaakt door medewerkers. Samen met de gevoeligheid van financiële instellingen zoals banken maakt deze toetsing belangrijk. Op deze manier kan nieuwe kennis toegevoegd worden aan bestaande kennis en behalen andere organisaties hier hun voordelen mee.

Om het vervolgonderzoek te concretiseren en ervoor te zorgen dat er nieuwe kennis aan de bestaande kennis kan worden toegevoegd worden o.a. de volgende individuele variabelen vertrouwen en leeftijd toegevoegd. Deze variabelen in combinatie met de verschillende medewerkers van een hoofdkantoor en een bijkantoor zodat tevens de differentiatie wordt

meegenomen. Door dit onderzoek uit te voeren middels een case study kunnen de resultaten uit het onderzoek worden vergeleken met de theorieën uit de bestaande literatuur. Hierdoor krijgen we een aanvulling op belangrijke aspecten van ISA, welke factoren omtrent ISA een belangrijke rol binnen de financiële dienstverlening spelen, de verschillen van ISA tussen medewerkers van het hoofdkantoor en bijkantoor, welke factoren van invloed zijn op informatiebeveiligingsgedrag, welke bewustmakingscampagnes eventueel kunnen bijdragen aan ISA en tot slot antwoord op de vraag of een ISA-programma wordt beïnvloed door de verschillen tussen medewerkers van het hoofdkantoor en de medewerkers van een bijkantoor.

3. Methodologie

Dit hoofdstuk gaat in op de methodologie en bestaat uit het conceptueel ontwerp, technische ontwerp en de methode voor het verzamelen van de gegevens. Dit hoofdstuk eindigt met een reflectie waarin de validiteit, betrouwbaarheid en ethische aspecten van het onderzoek worden weergegeven.

3.1. Conceptueel ontwerp

Case study

Zoals eerder aangegeven wordt het empirische onderzoek uitgevoerd middels een case study. Op deze manier kan de theorie uit de bestaande literatuur vergeleken worden binnen de financiële dienstverlening. De case study valt normaliter onder een kwalitatieve onderzoeksmethode en heeft de volgende centrale definitie: "*een case study heeft de noodzaak om een evenement of fenomeen diepgaand en in zijn natuurlijke context te verkennen"* (Lewis, Saunders, & Thornhill, 2019). Daarnaast zijn er drie hoofdtypen; intrinsiek, instrumenteel en collectief. Een intrinsieke case study wordt meestal ondernomen om te leren over een uniek fenomeen. De instrumentele casus daarentegen gebruikt één bepaalde situatie "geval" om een bredere waardering van een probleem te krijgen. De collectieve case study omvat het bestuderen van meerdere "gevallen" tegelijkertijd. (Stake, 1995). Dit onderzoek wordt uitgevoerd middels een instrumentele casus, waarbij het leren over een probleem, gebeurtenis of fenomeen centraal staat en er na afronding van het empirische onderzoek nieuwe kennis aan bestaande kennis toegevoegd. Bij een instrumentele case hoort een kritische aanpak, de onderzoeker stelt eigen en andermans aannamen ter discussie. Dit betreft een van de voordelen. Een ander onderscheid hangt samen met de complexiteit van de "gevallen" die worden bestudeert: Een eenheid op zich wordt aangeduid als een holistisch design. Indien deze uit meerdere elementen bestaat wordt dit aangeduid als embedded design. Uit deze genoemde methodes kunnen de volgende combinaties ontstaan: Enkelvoudig holistisch, enkelvoudig embedded, meervoudig holistisch of meervoudig embedded (Yin, 2014). Dit onderzoek wordt uitgevoerd middels een enkelvoudig embedded design. De case als geheel bestaat uit meerdere elementen doordat het verschil wordt onderzocht tussen een bijkantoor en het hoofdkantoor. Om uiteindelijk inzicht te krijgen worden deze afzonderlijk bestudeerd. Voordelen van een case study zijn o.a. het gedetailleerd onderzoeken waardoor de gegevens rijker en diepgaander zijn. Daarnaast richt een case study zich op een brede probleemstelling waardoor er vernieuwde inzichten kunnen worden verkregen. Een nadeel van een case study is dat dit vaak door één onderzoeker wordt uitgevoerd waardoor het achterhalen van een duidelijke oorzaak-gevolg relatie lastiger is.

Mede wegens het recente onderzoek wat gehouden is binnen dezelfde groot bank is er bewust gekozen om de kwalitatieve gegevens uit dit onderzoek te gebruiken als basis voor een onderzoek waarbij bevindingen worden gevalideerd middels kwantitatief onderzoek. Hierbij wordt gebruik gemaakt van de "mono method quantitative" methode. Deze methode kenmerkt zich door het gebruik van één type methode namelijk kwantitatief. Kwantitatief onderzoek wordt over het algemeen geassocieerd met een deductieve benadering, de focus ligt hierbij op het gebruik van data om een specifieke theorie te toetsen. Deze methode verkent de relaties tussen variabelen waarna ze

numeriek worden gemeten en geanalyseerd met behulp van statistische technieken. (Saunders, Lewis, & Thornhill, 2019) Gezien de beperkte tijd voor het afronden van dit onderzoek wordt deze cross-sectioneel uitgevoerd. Dit houdt in dat de meting van het fenomeen op een bepaald moment betrokken is. Het empirische onderzoek kent de volgende fases: vooronderzoek, documentenanalyse en kwantitatief onderzoek.

3.2. Technisch ontwerp: uitwerking van de methode

Het onderzoek wordt uitgevoerd binnen de sector financiële dienstverlening, organisatie Bank X. Er worden twee groepen gemaakt: de medewerkers van het hoofdkantoor en medewerkers van een bijkantoor. Om antwoord te krijgen op de hoofdvraag is het van belang dat er binnen een financiële instelling data wordt verzameld over Security Awareness Information (ISA), de onderdelen van ISA, welke factoren van belang zijn, de verschillen tussen een hoofd en bijkantoor, welke factoren van invloed zijn op informatiebeveiligingsgedrag, welke campagnes een bijdrage leveren aan informatiebeveiligingsgedrag en tot slot de validatie op de bevindingen van het onderzoek uitgevoerd door Noury Takens (Takens, 2020). Om de kwaliteit van de onderzoeksresultaten te waarborgen wordt er gebruikgemaakt van gecombineerde dataverzamelingstechnieken. Hieronder volgt een omschrijving.

Documentenanalyse

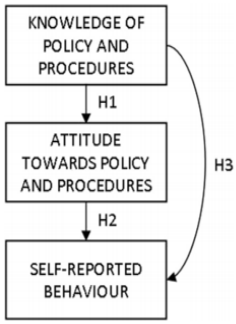
Om de huidige situatie te analyseren wordt er een interne documentenanalyse toegepast. De documentenanalyse betreft een kwalitatieve dataverzamelingstechniek. Indien de organisatie waar het empirische onderzoek wordt uitgevoerd gebruik maakt van intranet, start de analyse hier. Op basis van de gevonden informatie wordt er nieuwe data verkregen. Om rekening te houden met de hoeveelheid informatie worden de documenten geselecteerd op basis van de volgende zoektermen: Informatiebeveiliging, Cybersecurity, Handleiding medewerkers en Jaarverslag.

Enquête

De documentatieanalyse wordt gecombineerd met een enquête. De gekozen methodiek heeft meestal het karakter van een deductieve onderzoeksaanpak. Op deze manier is het mogelijk om een grotere groep te bereiken waardoor de representativiteit van het onderzoek wordt verhoogd mits er sprake is van een hoog respons. De enquêtevragen worden opgesteld aan de hand van de documentatieanalyse, het eerder gehouden groepsinterview en de vragenlijst R-HAIS-Q. De vragen bestaan uit meerkeuzevragen waardoor de statistische analyse wordt vergemakkelijkt door de standaardisatie. De enquête wordt ingezet binnen zowel het hoofdkantoor als binnen de bijkantoren. Hierbij wordt rekening gehouden met een eerder onderzoek binnen bank X, tevens gehouden omtrent het onderwerp ISA. Om ervoor te zorgen dat respondenten niet twee keer worden benaderd wordt de enquête uitgezet bij de volgende bijkantoren: Rotterdam, Delft, Drechtsteden, Voorneputten, Den Haag en Amsterdam. Binnen de bijkantoren zijn dit de afdelingen: Accountmanagers Midden en kleinbedrijf (MKB), Financieel adviseurs (FA) en Private Bankers (PB). Dit betreft een gemiddelde van 60 respondenten per bijkantoor. Er is bewust voor deze afdelingen gekozen vanwege de kenmerken van een bijkantoor: dit betreffen respondenten met direct klantcontact. Binnen het hoofdkantoor worden de volgende afdelingen benaderd: Credit Analysis, Data Management, Dimensions Operations, Food and Agri, HR en Global monitoring. Deze afdelingen zijn bewust gekozen doordat men niet direct klantcontact heeft.

HAIS-Q

Zoals eerder aangegeven is HAIS-Q een meetinstrument die ISA beoordeelt op zeven belangrijke gebieden waaronder wachtwoordbeheer, e-mailgebruik, internetgebruik, gebruik van sociale media, beveiliging van mobiele apparaten, informatieverwerking en incidentrapportage. Hierbij wordt elk aspect onderzocht op kennis, houding en gedrag (Butavicius, Jerram , McCormac , Parsons , & Pattinson , 2014). De componenten van het KAB model worden in figuur 2 weergegeven.



Figuur 2. KAB-component van het HAIS-model

De originele HAIS-Q is te vinden in bijlage 2. De HAIS-Q vragenlijst wordt aangepast aan de onderzoeksvraag en de doelgroep. Daarnaast is het van belang om de bevindingen van eerder onderzoek te valideren, om de bevindingen uiteindelijk met elkaar te kunnen vergelijken wordt de R-HAIS-Q als basis gebruikt (Takens, 2020). De R-HAIS-Q bestaat uit de volgende aandachtsgebieden: Wachtwoordbeheer, gebruik van e-mail, gebruik van sociale media, mobiele apparaten en rapportage van incidenten. Dit resultaat komt voort uit het focusgroep-interview (Takens, 2020). De vragen vanuit de R-HAIS-Q worden aangevuld met vragen over het e-mailcontact met onbekende partijen van zowel medewerkers van een bijkantoor als de medewerkers van het hoofdkantoor. Een belangrijke toevoeging aan de vragenlijst is het focusgebied vertrouwen zodat er een eventueel verband met ISA wordt achterhaald. De toevoeging van een extra aandachtsgebied wordt aangeraden door (Butavicius, Jerram , McCormac , Parsons , & Pattinson , 2014). Op deze manier wordt de duurzaamheid van de HAIS-Q-methode gewaarborgd. De vragenlijst bestaat uit 33 gesloten vragen. Deelnemers krijgen de instructie om op elk item te reageren op een vijfpuntsschaal van "Helemaal niet mee eens" tot "Helemaal mee eens". Op deze manier worden de nieuwe waardes meegenomen om te bepalen of dit invloed heeft op ISA binnen de financiële dienstverlening. De vragenlijst wordt uitgezet middels LimeSurvey (https://www.limesurvey.org).

3.3. Gegevensanalyse

Om de verkregen data te analyseren is het van belang dat er een analyseplan wordt opgesteld. Een onderscheid tussen de twee categorieën is noodzakelijk gezien deze beide een verschillende manier van analyse vergt. De methode voor de gegevensanalyse wordt als volgt weergegeven:

Analyse van kwantitatieve data

De analyse van kwantitatieve data betreft in dit onderzoek specifiek de analyse van de uitkomsten uit het onderzoek. Deze data vergt een statistische analyse waarbij er gebruikt wordt gemaakt van het softwareprogramma SPSS. Er worden voorafgaand de statistische analyse een aantal stappen genomen. De start van de analyse begint met het controleren van de datamatrix, om fouten te voorkomen is het van belang dat alle data in de juiste kolommen zijn weergegeven. Vervolgens worden frequenties uitgedraaid. Om ervoor te zorgen dat de gevonden data aan de analysetechnieken voldoen wordt er gekeken naar het gemiddelde, de spreiding, de modus, de mediaan en scheefheid. Tevens worden de variabelen onderscheiden in de volgende twee soorten: onafhankelijke variabelen: dit ligt vast, maar veroorzaakt een verandering en afhankelijke variabele: verandert onder invloed van de onafhankelijke variabele. Met de analyse van de kwantitatieve data worden de verschillende groepen vergeleken en bevindingen uit het onderzoek van Noury Takens gevalideerd.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Hieronder wordt de reflectie t.a.v. validiteit en betrouwbaarheid weergegeven, dit stuk eindigt met een korte toelichting over de ethische aspecten van het onderzoek. Bij de discussie van het onderzoek wordt hiernaar gerefereerd. Het is van groot belang om deze aspecten zo hoog mogelijk te krijgen, echter is een percentage van 100% niet haalbaar. Volgens Yin zijn er vier criteria waarbij een verschijnsel getoetst kunnen worden: interne validiteit, externe validiteit, construct validiteit en betrouwbaarheid (Yin, 2014).

Interne validiteit
De interne validiteit in een onderzoek betreft de mate waarin het redeneren juist is uitgevoerd. Hoe kleiner de kans op verwarring of disputatie hoe hoger de interne validiteit van een onderzoek. Om de interne validiteit te verhogen dienen alternatieve verklaringen voor bevindingen uitgesloten te worden. Om de interne validiteit van dit onderzoek te verhogen wordt er gebruik gemaakt van triangulatie, dit houdt in dat er meerdere bronnen worden gebruikt om constateringen te toetsen. Zo wordt er gestart met deskresearch gevolgd door een enquête. Daarnaast is er tijdens het literatuuronderzoek al gebruik gemaakt van meerdere methodes en theorieën.

Externe validiteit
De externe validiteit in een onderzoek is de mate waarin de uitkomst van een onderzoek toepasbaar is bij eventuele andere bedrijven, instellingen of sectoren. Ofwel de “generaliseerbaarheid” van het onderzoek. Om dit te toetsen kan onderzocht worden of het onderzoek dezelfde resultaten zouden opleveren indien dit op een ander tijdstip, andere plaats of in een andere organisatie met andere medewerkers wordt uitgevoerd. Gezien het onderzoek wordt gehouden binnen de financiële sector is het belangrijk dat er goed gekeken wordt naar de populatie van de respondenten. Er kan achteraf een steekproef gehouden worden of relevante kenmerken lijken op de populatie. Daarnaast is er tijdens het literatuuronderzoek niet alleen gebruik gemaakt van theorieën binnen de financiële sector, de literatuur is hierbij in brede zin onderzocht. Dit laatste is belangrijk vanwege de casestudy als onderzoeksopzet, de theorie wordt getoetst in de praktijk.

Constructvaliditeit
Constructvaliditeit in een onderzoek gaat over de mate waarin een test of meting het beoogde doel beantwoordt. Het gaat hier net als externe validiteit om het generaliseren. Het verschil met externe validiteit is dat het bij constructvaliditeit van belang is dat er gekeken wordt naar bedoelt “begrip”. Zo is het bijvoorbeeld lastig om meningen en emoties te meten. Om hier rekening mee te houden worden er in de enquête meerdere vragen gesteld over één begrip en worden de vragen zo goed mogelijk geformuleerd zodat er geen verwarring kan ontstaan. Statistisch gezien kan de constructvaliditeit vervolgens worden aangetoond middels het uitvoeren van de factoranalyse.

Betrouwbaarheid
De betrouwbaarheid in een onderzoek betreft de mate waarin de onderzoeksmethode stabiele en consistente resultaten oplevert. Zo wordt een specifieke meting als betrouwbaar beschouwd indien de toepassing ervan op hetzelfde meetobject dezelfde resultaten oplevert. Hoe groter de kans dat de resultaten uit onderzoek op toeval berusten, hoe lager de betrouwbaarheid. Om de betrouwbaarheid in dit onderzoek te verhogen wordt er een logboek bijgehouden, hierdoor wordt er inzichtelijk gemaakt hoe de onderzoeksgegevens zijn verkregen en kan een andere onderzoeker eenvoudig hetzelfde onderzoek herhalen. Dit wordt ook wel intrabeoordelaarsbetrouwbaarheid genoemd en kan statistisch gezien ook gemeten worden door het gebruik van SPSS. Als onderzoeker is het tevens mogelijk om achteraf te concluderen dat sommige behaalde resultaten niet worden

meegenomen in het onderzoek vanwege de inconsistentie. Zo worden de resultaten van het onderzoek zo betrouwbaar mogelijk gehouden.

Ethische aspecten

Om de wetenschappelijke integriteit in het onderzoek te waarborgen is het van belang dat er rekening wordt gehouden met ethiek, we hebben immers te maken met de mens en maatschappij. Wetenschappelijk onderzoek naar gedrag of beleid is vaak moeilijk los te koppelen van normatieve (voor)oordelen over het gedrag en beleid. Daarnaast betreft het met name het respecteren van menselijke waardigheid, wetenschappelijke validiteit en wetenschappelijke of educatieve relevantie. De enquêtes worden alleen gehouden en beschreven na toestemming van de respondent, om de privacy van de respondent te waarborgen worden zij in het onderzoek niet bij naam genoemd. Het verwerken van de persoonsgegevens is in lijn met de Algemene verordening gegevensbescherming (AVG), zo worden alleen gegevens verwerkt die noodzakelijk zijn om het doel van het onderzoek te behalen. Daarnaast worden de gegevens verwijderd zodra het onderzoek is afgerond en het onderzoek is geverifieerd. Tevens worden de richtlijnen van de Nederlandse Gedragscode Wetenschappelijke integriteit gevolgd. Hierbij gaat het om betrouwbaarheid, zorgvuldigheid, onpartijdigheid, controleerbaarheid, en onafhankelijkheid van onderzoek. Verzamelde data wordt zorgvuldig en zo transparant mogelijk beschreven en om onpartijdigheid te borgen worden er geen enquêtes afgenomen met respondenten met een functionele of hiërarchische relatie van de onderzoeker.

4. Resultaten

Dit hoofdstuk staat stil bij de uitvoering van het onderzoek, de respons verkregen uit de X-HAIS-Q en de resultaten op de eerder geformuleerde hypothesen.

4.1. Uitvoering van het onderzoek

De start van het empirische onderzoek is begonnen met het verzamelen van een grote hoeveelheid academische literatuur op het gebied van ISA. Dit heeft geresulteerd in een aantal hypothesen, middels het verzamelen van gegevens door een enquête wordt er antwoord gegeven op de hypothesen.

Respondenten

De R-HAIS-Q in het onderzoek van Noury is uitgezet onder 365 medewerkers waarvan 71 medewerkers de enquête (R-HAIS-Q) daadwerkelijk hebben ingevuld. Om de validiteit en betrouwbaarheid van het onderzoek vergelijkbaar te houden is het essentieel om minimaal hetzelfde aantal respondenten aan te houden. Om deze reden is de enquête uitgezet onder 468 medewerkers. Om te voorkomen dat dezelfde medewerkers ondervraagd worden is er onderzocht welke medewerkers van welke bijkantoren en welke afdelingen reeds eerder zijn ondervraagd in het onderzoek van Noury. Deze respondenten worden geen tweede keer verzocht om de enquête in te vullen.

Gegevensanalyse

Aangezien er twee onafhankelijke groepen worden vergeleken; namelijk de medewerkers van bijkantoren en de medewerkers van het hoofdkantoor, is er een statistische toets benodigd die de gemiddelden van 2 onafhankelijk groepen vergelijkt. Uit onderzoek blijkt dat er bij het vergelijken van onafhankelijke groepen zowel gebruik kan worden gemaakt van de t-test als de Mann-Whitney U test. Voor de vijfpunts-Likert items, hebben de t-test en de Mann-Whitney U test over het algemeen een vergelijkbaar vermogen op analyse (de Winter & Dodou, 2010). In dit onderzoek wordt gebruik gemaakt van de Mann-Whitney U test zodat de gegevens eenvoudig te vergelijken zijn met de resultaten uit het eerder gehouden onderzoek. Alvorens de statische toets wordt uitgevoerd wordt er gekeken naar de scores op Knowledge, Attitude en Behavior niveau en het niveau van ISA tussen de medewerkers van het hoofdkantoor en de medewerkers van een bijkantoor. De weergaven van de resultaten zorgen uiteindelijk voor de beantwoording op de hoofd en deelvragen.

4.2. Enquête X-HAIS-Q

Om ervoor te zorgen dat de resultaten uit het eerder gehouden onderzoek van Noury eenvoudig vergeleken en gevalideerd kunnen worden is er gekozen om de R-HAIS-Q als basis voor de X-HAIS-Q te gebruiken. De R-HAIS-Q bestaat uit de volgende aandachtsgebieden: Wachtwoordbeheer, gebruik van e-mail, gebruik van sociale media, mobiele apparaten en rapportage van incidenten. Dit resultaat komt voort uit het focusgroep-interview (Takens, 2020). De X-HAIS-Q heeft het aandachtsgebied vertrouwen als nieuwe toevoeging. Daarnaast wordt er niet alleen getoetst op contact met klanten maar tevens met externe partijen zoals leveranciers, tussenpersonen, accountants en verzekeringsmaatschappijen. Deze toevoeging vloeit voort uit een aanbeveling waarop beide groepen e-mailcontact hebben met onbekende afzenders. De vragenlijst is gemaakt met hulp van LimeSurvey (https://www.limesurvey.org). Om ervoor te zorgen dat de respondenten geen andere enquête ontvangen en hierdoor vragen anders kunnen interpreteren is er gekozen voor dezelfde opzet als de R-HAIS-Q. Dit houdt in dat er per set van vragen een korte uitleg wordt gegeven over Knowledge, Attitude en Behavior. Als aanvulling op de 45 stellingen zijn de volgende algemene vragen gesteld: geslacht, leeftijd, opleidingsniveau en werkomgeving. Daarnaast zijn er 4 stellingen over het vertrouwen in de technologie aangeboden. Bij elke stelling was het mogelijk om

de optie 'geen antwoord' of 'niet van toepassing' te selecteren. Om rekening te houden met het internationale karakter binnen de financiële dienstverlening is de voertaal van de enquête Engels.

Respons
Om een zo hoog mogelijke respons te realiseren is rekening gehouden met de aanbevelingen vanuit de literatuur (Saunders, Lewis, & Thornhill, 2019). Zo is er vermeld hoeveel tijd het invullen van de enquête in beslag neemt, heeft de enquête een duidelijke lay-out, wordt de enquête anoniem afgenomen, is er uitleg bij lastige vragen weergegeven en is er na 10 dagen een reminder verstuurd inclusief vermelding van de datum waarop de enquête sluit. Ondanks een betrouwbaarheidsniveau van 90%, 95% en 99% gebruikelijk is ten aanzien van de steekproefgrootte, geeft de literatuur ook weer dat vandaag de dag een respons van minder dan 10% niet ongewoon is voor een online enquête (Couper, Kapteyn, Schonlau, & Winter, 2007).
De enquête X-HAIS-Q is uitgezet op 22 oktober 2020 en op 1 november 2020 is een reminder verzonden waarbij is aangegeven dat men tot 6 november 2020 de tijd heeft om de enquête in te vullen. 6 november was dan ook de daadwerkelijke sluitingsdatum. In totaal hebben 87 respondenten de enquête ingevuld waarvan 60 volledig en 27 onvolledig. 87 respondenten betreft op een steekproefgrootte van 468 medewerkers 19.02 %, echter wordt de onvolledig ingevulde respons niet meegenomen in de resultaten, conclusie en aanbevelingen.

Analyse onvolledige respons
Zoals reeds eerder genoemd hebben 27 respondenten een onvolledig respons gegeven. Om toch een beeld te geven over deze groep wordt hieronder in hoofdlijnen weergegeven wat de respondenten wél hebben ingevuld.

- 4 respondenten hebben de enquête wel geopend maar direct gesloten, hierbij is geen antwoord op een vraag ingevuld. Dit houdt in dat er nog 23 respondenten overblijven voor verdere analyse.
- Meer dan de helft van de respondenten zijn werkzaam voor een bijkantoor, dit zijn er om precies te zijn 16, 5 respondenten zijn werkzaam op het hoofdkantoor en 2 respondenten hebben “geen antwoord” aangegeven.
- 12 van de 23 respondenten heeft alleen de algemene vragen ingevuld, wat impliceert dat men gestopt is zodra de KAB stellingen inclusief de 5 punts-Likertschaal aanbod kwamen.
- 11 respondenten hebben de 16 kennisstellingen (Knowledge van KAB) ingevuld. Er blijven hierna nog 6 respondenten over voor verdere analyse. De 6 respondenten hebben de 17 houdingstellingen (Attitude van KAB) ingevuld en zijn gestopt zodra de set met 17 stellingen over gedrag (Behavior van KAB) aanbod kwam.

Analyse volledige respons
In totaal zijn er 60 respondenten die de enquête volledig hebben ingevuld. Voordat er een conclusie uit deze resultaten wordt getrokken is het van belang dat er accuraat naar de respons wordt gekeken.

- Alle 60 respondenten zijn of werkzaam bij een bijkantoor óf werkzaam voor het hoofdkantoor. De verdelingen tussen deze populatie is 31 en 29, dit geeft een evenredig beeld waardoor er geen respondenten worden uitgesloten.
- Er wordt niet alleen wordt getoetst op contact met klanten maar tevens op contact met externe partijen zoals leveranciers, tussenpersonen, accountants en verzekeringsmaatschappijen. 45 respondenten geeft aan dagelijks contact te hebben met externe partijen, 15 respondenten geeft aan geen contact te hebben met externe partijen en 2 respondenten hebben aangegeven “geen antwoord”.
- 31 respondenten heeft aangegeven werkzaam te zijn voor het hoofdkantoor, 17 van hen heeft daarbij ook aangegeven dagelijkst contact te hebben met externe partijen. Ondanks dit een vertekend beeld kan geven om de verschillen van ISA tussen medewerkers van een

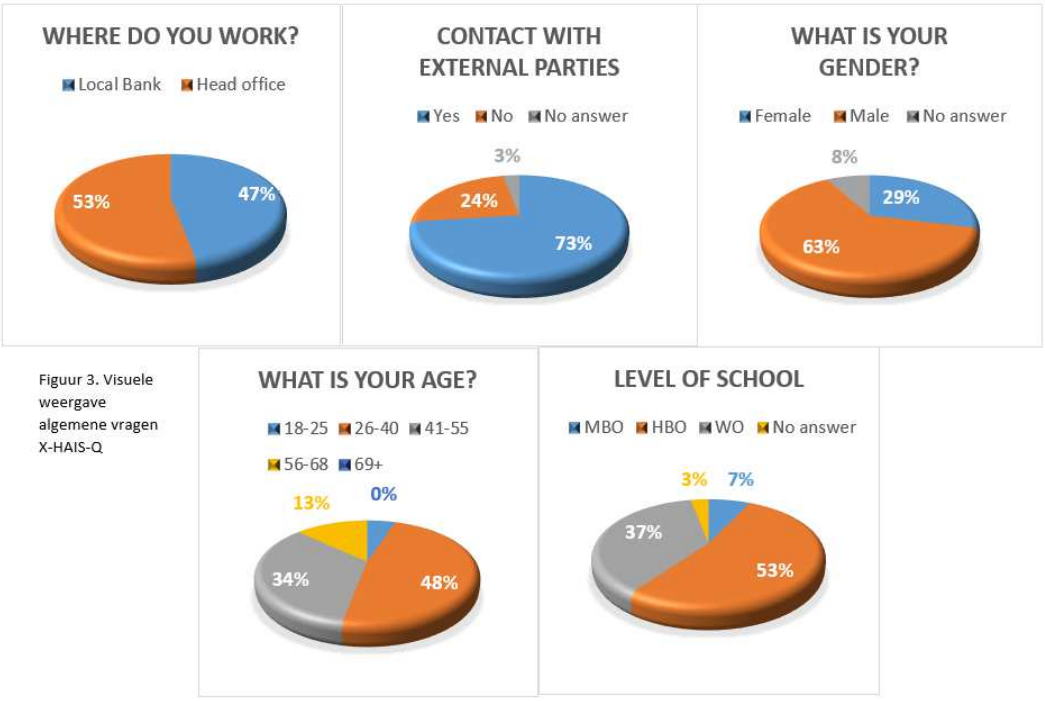
bijkantoor en een hoofdkantoor te weergeven is er bewust gekozen om de 17 respondenten binnen de sample te houden. De reden hiervan is dat we mogen aannemen dat het hier niet gaat om contact met particulieren maar met externe professionals van grote organisaties zoals accountants en verzekeringsmaatschappijen.

- Er is geen respondent die overal hetzelfde antwoord heeft gegeven, hierbij mogen we aannemen dat iedere respondent de antwoorden accuraat heeft ingevuld.

4.3. Enquête X-HAIS-Q resultaten

In 4.3. worden de enquête X-HAIS-Q resultaten weergegeven. Eerst wordt er een globaal beeld van de respondenten weergegeven, vervolgens de betrouwbaarheid van de enquête gevolgd door de ISA meeting en eindigend in de verschillen tussen de groepen. De vragen en antwoorden zijn in het Engels weergegeven zodat er geen interpretatie verschillen kunnen ontstaan en de percentages zijn afgerond indien er sprake is van meerdere decimalen achter de komma. Tevens wordt de invulling van “geen antwoord” alleen aangegeven indien hier daadwerkelijk sprake van is.

Algemene informatie respondenten



Figuur 3. Visuele weergave algemene vragen X-HAIS-Q

Zoals reeds eerder aangegeven betreft het een verdeling van bijna 50/50 tussen respondenten van een bijkantoor en respondenten van het hoofdkantoor. Door de aanpassing van de vraag of men contact heeft met externe partijen is te zien dat ongeveer ¾ van de respondenten hier het antwoord “ja” heeft gegeven. Het grootste deel van de ondervraagden zijn mannen, bijna de helft heeft een leeftijd van 26 tot 40 jaar en iets meer dan de helft heeft een HBO diploma. 23 respondenten heeft een WO diploma waarvan 18 medewerkers op het hoofdkantoor en 5 medewerkers op een bijkantoor.

Betrouwbaarheid X-HAIS-Q

Om de interne consistentie van de stellingen van X-HAIS-Q te meten is er gebruik gemaakt van de berekening conform de Cronbach’s Alpha in SPSS. De Cronbach’s Alpha is toegepast op ISA in het algemeen, de KAB dimensie en de vijf verschillende aandachtsgebieden. Dit geeft een indicatie van de gemiddelde correlatie tussen alle items die deel uitmaken van de weegschaal ofwel: wordt er getoetst wat we beogen te toetsen? (Pallant , 2007) beveelt een minimumniveau aan van 0,7. echter wordt er ook aangegeven dat de waarden afhankelijk zijn van het aantal items in de Schaal.

Wanneer er sprake is van een klein aantal items (minder dan 10) kunnen de waarden laag zijn. In deze situatie wordt genoegen genomen met een minimumniveau van 0,5 (Pallant , 2007)
De resultaten worden weergegeven in Figuur 4. De algemene score van ISA voldoet aan de vereiste waarde van 0,7. Zoals te zien scoort de KAB dimensie Knowledge ver onder de vereiste waarde van 0,7 ondanks er meerdere items zijn verwijderd. Een verklaring zou kunnen zijn dat de vragen over de onderwerpen te veel van elkaar verschillen waardoor de vragen niet consistent zijn beantwoord. Desondanks kunnen we geen betrouwbare conclusies trekken uit de KAB dimensie Knowledge, deze wordt dan ook niet meegenomen in het berekenen van de ISA-score later in dit hoofdstuk.

Om de betrouwbaarheid te verhogen zijn in totaal twee items verwijderd, één voor de KAB dimensie Attitude en één voor de KAB dimensie Behavior, dit is gedaan om de minimale waarde van 0,7 te behalen. Voor een overzicht van de desbetreffende verwijderde de items in Figuur 5. Figuur 6 geeft de uitkomsten weer van de Cronbach's Alpha per aandachtgebied, doordat deze is berekend conform de theorie van (Pallant , 2007) was het verwijderen van items niet nodig gezien hier het behalen van minimaal 0,5 voldoende wordt geacht.

Figuur. 4. Cronbach's Alpha per Dimensie en algemene ISA

Cronbach's Alpha	Output
Knowledge	.411
Attitude	.508
Behavior	.652
Algemeen ISA	.765

Cronbach's Alpha per Dimensie incl. verwijdering items

Cronbach's Alpha na verwijdering items	Output
Knowledge	.411
Attitude	.693
Behavior	.708
Algemeen ISA	.765

Figuur 5. Verwijderde items

Code	Dimensie	Item
ATP01	Attitude	It's safe to use the same password for social media and work accounts.
BES07	Behavior	I don't regularly review my social media privacy settings.

Figuur 6. Cronbach's Alpha per aandachtsgebied

Cronbach's Alpha per aandachtsgebied	Output
Password management	.517
Email use	.737
Social media use	.551
Mobile devices	.607
Incident reporting	.518

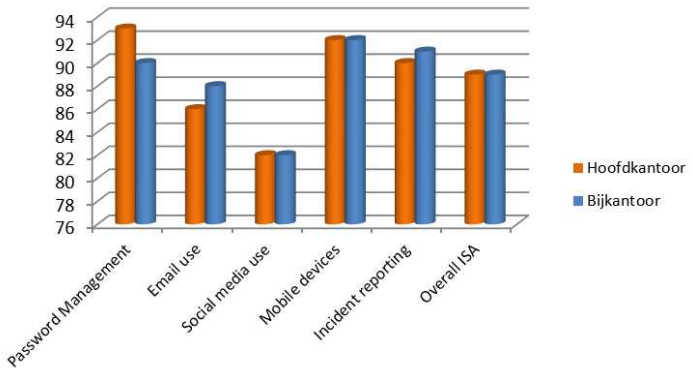
ISA score en verschillen tussen hoofdkantoor en bijkantoor
Uit diverse literatuurstukken zoals (Butavicius, et al., 2017) is de mate van information security awareness berekend middels de volgende formule: $ISA\ \% = \frac{SA + A}{n}$
Hierbij staat SA voor antwoorden die worden ingevuld met "Strongly Agree", A staat voor "Agree" en "n" zijn het totaal aantal ingevulde antwoorden. De formule is toegepast op zowel KAB dimensie (zonder K gezien de lage Cronbach's Alpha waarde) als de aandachtgebieden. Om het verschil tussen de medewerkers van het hoofdkantoor en bijkantoor te vergelijken worden de resultaten apart van elkaar weergegeven zodat een eventueel verschil direct zichtbaar is.

Figuur 7. ISA score per dimensie, aandachtsgebied en locatie kantoor

Medewerkers van het hoofdkantoor	Attitude	Behavior	ISA
Password Management	90	95	93
Email use	92	79	86
Social media use	88	76	82
Mobile devices	94	89	92
Incident reporting	95	85	90
Totaal	92	85	89

Medewerkers van het bijkantoor	Attitude	Behavior	ISA
Password Management	87	92	90
Email use	89	86	88
Social media use	82	82	82
Mobile devices	93	91	92
Incident reporting	94	88	91
Totaal	89	88	89

Figuur 8. Visuele weergave ISA score



Zoals weergeven in figuur 7 en 8 scoren de medewerkers van het hoofdkantoor hoger op de aandachtgebieden Password Management en Email use. Er worden geen verschillen waargenomen voor Social media use en Mobile devices en de medewerkers van het bijkantoor scoren hoger op Incident reporting. De verschillen in het aandachtsgebied Password Management zijn het grootst, de overall score van ISA in algemene zin blijft gelijk op 89.

Mann-Whitney U

Na het weergeven van de interne betrouwbaarheid middels de Cronbach's Alpha worden in deze paragraaf de eventuele significante verschillen gemeten tussen de medewerkers van het hoofdkantoor en de medewerkers van een bijkantoor. Om de verschillen waar te nemen wordt gebruik gemaakt van de Mann-Whitney U-test. Een aantal voordelen van het gebruik van deze test betreft o.a. dat gegevensverdeling van de populatie niet nodig is en de test goed mogelijk is voor een kleiner aantal samples (Nachar, 2008). De Mann-Whitney U test is uitgevoerd met behulp van SPSS, de testresultaten verschijnen uiteindelijk in twee verschillende tabellen. In de eerste tabel worden de waarden van de Rangen, de Gemiddelde Rang en de Som van Rangen weergegeven, de N geeft het aantal deelnemers weer. In de tweede tabel worden de resultaten van de test weergegeven middels Mann-Whitney U, Wilcoxon W, Z en Asymp. Sig. (2-staart). Asymp. Sig (2-staart) is voor de analyse het meest belangrijk, als de waarde lager is dan .05, kan worden geconcludeerd dat er is een statistisch significant verschil is gemeten (Nachar, 2008).
Een overzicht van de resultaten wordt weergegeven in figuur 9, de totale uitslag van de test is te vinden in bijlage 3. De items met een significant verschil worden in kleur van de groep aangegeven (in het voordeel), blauw betreft het bijkantoor en oranje het hoofdkantoor. In onderstaand overzicht worden de items met het betreffende significante verschil weergegeven, onder het overzicht gaan we dieper in op de resultaten.

		Hoofdkantoor			Bijkantoor			Testresultaten			
KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Whitney U	Wilcoxon W	Z	Asymp. Sig.
Password Management											
A	It's safe to use the same password for social media and work accounts.	33	34,58	1141,00	28	26,79	750,00	344,000	750,000	-1,900	,057
A	It's a bad idea to share my work passwords, even if a colleague asks for it.	33	28,15	929,00	28	34,36	962,00	368,000	929,000	-2,039	,041
Social Media use											
A	It's risky to post certain information about my work on social media.	32	35,47	1135,00	28	24,82	695,00	289,000	695,000	-2,625	,009

Password Management

Voor het aandachtsgebied Password Management zien we de volgende significante verschillen:

- It's safe to use the same password for social media and work accounts. De test geeft aan dat medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) beter scoren dan de medewerkers van een bijkantoor. Ofwel: medewerkers van het hoofdkantoor achten het minder veilig om hetzelfde wachtwoord voor zowel een social media, als werkaccount te gebruiken. Dit resultaat laat zich zien door de volgende gegevens: Mean Rank: 34,58 (H) / 26,79 (B), Whitney U: 344, Z -1,90 en een Asymp. Sig (tweestaart) van 0,57.
- It's a bad idea to share my work passwords, even if a colleague asks for it. De test geeft weer dat de medewerkers van een bijkantoor (op de KAB dimensie Attitude) beter scoren dan de medewerkers van het hoofdkantoor. Ofwel: medewerkers van een bijkantoor achten het minder veilig om een wachtwoord te delen met een collega, zelfs als deze collega er naar vraagt. Dit resultaat laat zich zien door de volgende gegevens: Mean Rank 28,15 (H) / 34,36 (B), Whitney U: 368, Z -2,03 en een Asymp. Sig (tweestaart) van 0,41.

Social Media use

Voor het aandachtsgebied Social Media use zien we het volgende significante verschil:

- It's risky to post certain information about my work on social media. De test laat zien dat de medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) beter scoren dan de medewerkers van een bijkantoor. Ofwel: de medewerkers van een bijkantoor vinden het minder risicovol om bepaalde informatie over werk op social media te plaatsen. Dit resultaat laat zich zien door de volgende gegevens: Mean Rank 35,47 (H) / 24,82 (B), Whitney U: 289, Z -2,62 en een Asymp. Sig (tweestaart) van 0,09.

Figuur 9. Resultaten Mann-Whitney U test Password Management en Social Media use

Password Management												
				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNP01	K	It's acceptable to use my social media passwords on my work accounts.	33	33,67	1111,00	29	29,03	842,00	407,000	842,000	-1,079	,280
2.	ATP01	A	It's safe to use the same password for social media and work accounts.	33	34,58	1141,00	28	26,79	750,00	344,000	750,000	-1,900	,057
3.	BEP01	B	I use a different password for my social media and work accounts.	32	30,98	991,50	29	31,02	899,50	463,500	991,500	-,008	,994
4.	KNP02	K	I am allowed to share my work passwords with my colleagues.	33	31,68	1045,50	29	31,29	907,50	472,500	907,500	-,165	,869
5.	ATP02	A	It's a bad idea to share my work passwords, even if a colleague asks for it.	33	28,15	929,00	28	34,36	962,00	368,000	929,000	-2,039	,041
6.	BEP02	B	I share my work passwords with colleagues.	33	29,98	989,50	29	33,22	989,50	428,500	989,500	-1,031	,303
7.	KNP03	K	A mixture of letters, numbers and symbols is necessary for my work passwords.	33	32,67	1078,00	29	30,17	875,00	440,000	875,000	-,622	,534
8.	ATP03	A	It's safe to have a work password with just letters.	33	31,64	1044,00	28	30,25	847,00	441,000	847,000	-,342	,732
9.	BEP03	B	I use a combination of letters, numbers and symbols in my work passwords.	33	29,39	970,00	27	31,85	860,00	409,000	970,000	-,620	,535

Social Media use													
				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNS07	K	I must periodically review the privacy settings on my social media accounts.	32	28,36	907,50	29	33,91	983,50	379,500	907,500	-1,294	,196
2.	ATS07	A	It's a good idea to regularly review my social media privacy settings.	31	29,44	912,50	28	30,63	857,50	416,500	912,500	-,300	,764
3.	BES07	B	I don't regularly review my social media privacy settings.	32	29,89	956,50	28	29,89	873,50	428,500	956,500	-,305	,760
4.	KNS08	K	I can't be fired for something I post on social media.	32	33,14	1060,50	29	33,14	830,50	395,500	830,500	-1,041	,298
5.	ATS08	A	It doesn't matter if I post things on social media that I wouldn't normally say in public.	32	31,67	1013,50	28	29,16	816,50	410,500	816,500	-,645	,519
6.	BES08	B	I don't post anything on social media before considering any negative consequences.	31	30,39	942,00	28	29,57	828,00	422,000	828,000	-,213	,831
7.	KNS09	K	I can post what I want about work on social media.	33	29,24	965,00	28	33,07	926,00	404,000	965,000	-1,078	,281
8.	ATS09	A	It's risky to post certain information about my work on social media.	32	35,47	1135,00	28	24,82	695,00	289,000	695,000	-2,625	,009
9.	BES09	B	I post whatever I want about my work on social media.	32	31,06	994,00	29	30,93	897,00	462,000	897,000	-,037	,970

4.4. Resultaat per hypothese

Tijdens de uitvoering van het literatuuronderzoek zijn er in totaal 6 hypothesen geformuleerd. In dit hoofdstuk worden de hypothesen bevestigd of ontkracht. Hypothesen 1, 2, 3.1 t/m 3.3 worden ontkracht en hypothese 4 heeft onvoldoende statistisch bewijs voor een significant resultaat. Hieronder volgt een uitgebreide analyse op de resultaten.

H1: Medewerkers van een hoofdkantoor volgen de ISA programma's beter op dan de medewerkers van een bijkantoor.
Uit het literatuuronderzoek naar ISA binnen de financiële dienstverlening bleek dat er onvoldoende bewijs is gevonden om de resultaten te generaliseren. Daarnaast is er voldoende belang bij toekomstig onderzoek op dit onderwerp. Om antwoord te geven op de hypothese en stil te staan bij de resultaten kan er het volgende worden meegegeven: de overall score van ISA voor zowel de medewerkers van het hoofdkantoor als de medewerkers van een bijkantoor blijft gelijk op 89. Zoals weergeven in figuur 7 en 8 scoren de medewerkers van het hoofdkantoor overall hoger op de aandachtgebieden Password Management en Email use. Om dieper in te gaan op het gedrag component (Behavior) blijkt dat de medewerkers van een bijkantoor beter scoren op de aandachtsgebieden Social Media use, E-mail use, Social media use, Mobile devices en Incident reporting. Alleen op het aandachtsgebied Password Management laten medewerkers van het hoofdkantoor een beter gedrag zien.

H2: De houding van medewerkers van een bijkantoor ten opzichte van het gebruik van sterke wachtwoorden is waarschijnlijk lager dan die van de medewerkers van het hoofdkantoor.
Uit het literatuuronderzoek is gebleken dat medewerkers van het hoofdkantoor een betere houding (A) aannemen ten aanzien van het gebruik van sterke wachtwoorden. Tegelijkertijd is er geen verschil waargenomen in de gerelateerde kennis- en gedragsverklaringen. Als antwoord op de hypothese kan het volgende resultaat worden weergegeven: overall laten de medewerkers van het hoofdkantoor een betere houding zien op het aandachtsgebied Password Management. Er is echter geen significant verschil conform de Mann-Whitney U test gevonden (in het voordeel van de medewerkers van het hoofdkantoor) op zowel de houding (A), gerelateerde kennis (K) en gedragsverklaringen (B) die erbij horen. Dit betreffen de items die specifiek ingaan op het gebruik van sterke wachtwoorden. Wel zijn er significante verschillen op andere items gevonden. Het resultaat wordt weergeven in figuur 9.

H3.1: De kennis van de medewerkers op een bijkantoor over de behandeling van e-mails van onbekende afzenders is waarschijnlijk hoger dan die van de werknemers op het hoofdkantoor.

H3.2: Medewerkers van een bijkantoor die kennis hebben van het aanklikken van links in e-mails van onbekende afzenders, zullen deze kennis waarschijnlijk niet in de praktijk brengen.

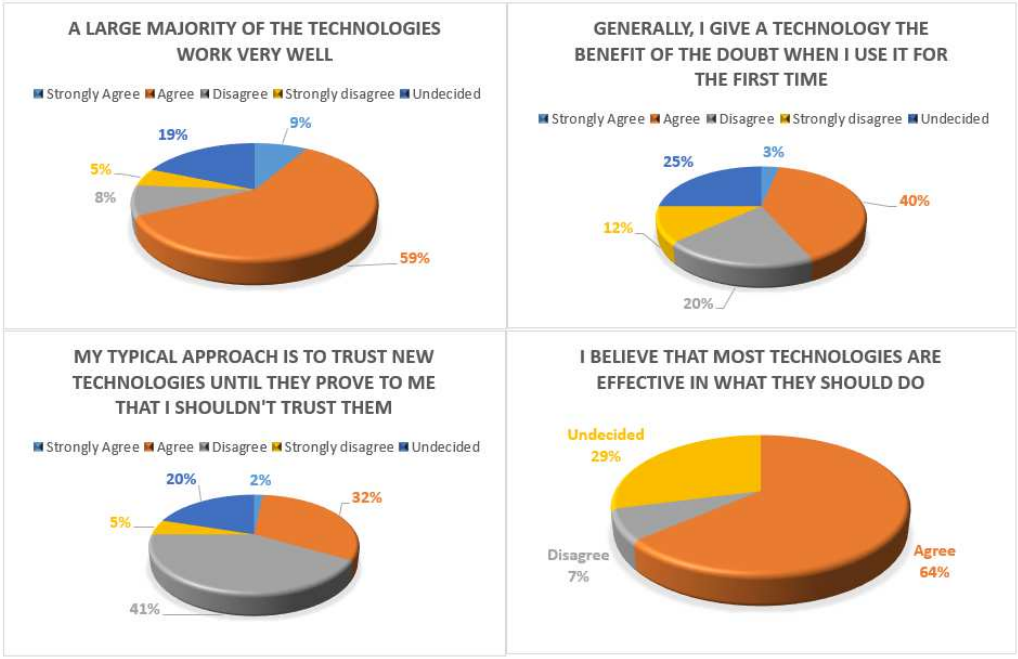
H3.3: Het is onwaarschijnlijk dat medewerkers van het hoofdkantoor kennis nodig hebben van het aanklikken van links in e-mails van onbekende afzenders om het gedrag te kunnen toetsen.
Uit het literatuur onderzoek zijn diverse bevindingen geconstateerd die gerelateerd zijn aan e-mails van onbekende afzenders. Medewerkers van een bijkantoor hebben een aanzienlijk betere kennis van het beleid en de procedures met betrekking tot klikken op links en het openen van bijlagen. Ondanks deze betere kennis laten zij dit niet zien in hun gedrag. Een beperking hierbij was dat men meerdere veronderstellingen niet heeft kunnen valideren, omdat men zich niet bewust was van de mate waarin de respondenten e-mailcontact hebben met onbekende partijen. In dit onderzoek is daar aandacht aan besteed. 45 van de in totaal 60 respondenten geeft aan dagelijks contact te hebben met externe partijen, 17 van hen is werkzaam bij het hoofdkantoor en 28 respondenten zijn werkzaam bij een bijkantoor. Er zijn echter geen significant verschillen gevonden op de items

conform de Mann-Whitney U test voor Hypothese 3.1, 3.2 en H3.3. Het resultaat wordt weergegeven in figuur 9.

H4: Medewerkers met vertrouwen in de technologie hebben positieve invloed op informatiebeveiligingsgedrag.

Uit het literatuuronderzoek is gebleken dat er in meerdere onderzoeken het element “vertrouwen” wordt genoemd. Vertrouwen is een belangrijke element in een digitale omgeving, desondanks is er weinig empirisch onderzoek gedaan naar de relatie tussen ISA en vertrouwen in de technologie. Het belangrijke element vertrouwen in de technologie in combinatie met de hoeveelheid uitgevoerde empirische onderzoeken binnen de financiële dienstverlening maakt op dat het van belang is om nieuwe kennis aan de bestaande kennis toe te voegen. In dit onderzoek zijn er 4 items aan de X-HAIS-Q toegevoegd om meer inzicht te krijgen in het fenomeen vertrouwen in de digitale omgeving. De items zijn niet meegenomen in de statistische toetsen doordat dit te weinig items zijn om er een significante conclusie uit te kunnen halen (Pallant , 2007). Om toch inzicht te geven worden de volgende resultaten weergegeven;

Figuur 10. Resultaten vertrouwen in de technologie



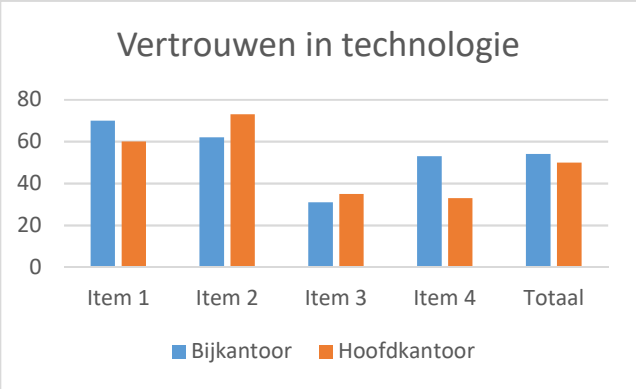
In totaal hebben 60 respondenten antwoord gegeven op de gestelde items. Opvallend is dat voor 3 van de 4 items meer dan de helft het eens is. Het item waarin een typische aanpak wordt voorgesteld geeft beduidend andere resultaten; 41% van de ondervraagden is het hier niet mee eens. Ook is gekeken of er een verschil aanwezig is tussen de medewerkers van het hoofdkantoor of de medewerkers van een bijkantoor. Doordat de items op dezelfde manier zijn geformuleerd als de ISA meeting is gekozen voor dezelfde formule waarbij de “Strongly Agrees” en “Agrees” worden gedeeld door het aantal respondenten. Deze resultaten worden weergegeven in figuur 11.
Hierin is te zien dat de medewerkers van een bijkantoor (op basis van de 4 gestelde items) een hoger vertrouwen in de technologie hebben dan de medewerkers van het hoofdkantoor. In figuur 12 worden dezelfde resultaten middels een visuele weergave aangegeven, hierin is te zien dat de grootste verschillen zijn gemeten op item nr. 4: de medewerkers van een bijkantoor geven vaker het voordeel van de twijfel als men een nieuwe technologie voor het eerst gebruikt. Zowel de medewerkers van een bijkantoor als de medewerkers van een hoofdkantoor scoren het laagst op item nr. 3: de aanpak om nieuwe technologieën te vertrouwen totdat ze het tegendeel bewijzen wordt dus minder vaak gehanteerd.

Figuur 11. Resultaten in vertrouwen in de technologie met een verschil tussen bijkantoor en hoofdkantoor

Item	Medewerkers van een bijkantoor	Score
1.	I believe that most technologies are effective in what they should do.	70
2.	A large majority of the technologies work very well.	62
3.	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	31
4.	Generally, I give a technology the benefit of the doubt when I use it for the first time.	53
	Totaal	54

Item	Medewerkers van het hoofdkanatoor	Score
1.	I believe that most technologies are effective in what they should do.	60
2.	A large majority of the technologies work very well.	73
3.	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	35
4.	Generally, I give a technology the benefit of the doubt when I use it for the first time.	33
	Totaal	50

Figuur 12. Visuele weergave resultaten in vertrouwen in de technologie



5. Discussie, conclusies en aanbevelingen

5.1. Discussie - reflectie

Uit eerder onderzoek naar ISA binnen 3 grootbanken is er differentiatie in groepen gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers. Medewerkers op een hoofdkantoor zijn vaker gefocust op het algemene beheer van een bank zonder klantcontact, denk aan compliance, projectmanagement en IT. De medewerkers op een bijkantoor hebben wel direct klantencontact. Deze onderscheidende profielen hebben sterke implicaties voor het beveiligingsgedrag (Bauer, 2017). Een belangrijk element ontbreekt in dit onderzoek, er is namelijk geen inzicht gegeven in het daadwerkelijke verschil op ISA niveau tussen de medewerkers van het hoofdkantoor of de medewerkers van een bijkantoor. Een later onderzoek binnen een grootbank in Nederland heeft nieuwe kennis toegevoegd (Takens, 2020). Na het uitzetten van een nieuwe versie van de HAIS-Q bleek namelijk dat er significante verschillen zijn tussen het hoofdkantoor en een bijkantoor specifiek binnen de aandachtsgebieden Wachtwoordbeheer, e-mailgebruik en gebruik van sociale media.

Om de resultaten uit eerder onderzoek te valideren en de betrouwbaarheid te verhogen is gekeken of bij herhaling van dit onderzoek, de resultaten hetzelfde zouden zijn en daarmee voldoende valide zijn. Om deze reden is de betreffende HAIS-Q als basis gebruik om vervolgens binnen dezelfde grootbank te verspreiden. De “X-HAIS-Q” is uitgezet onder 468 waarbij 60 respondenten de enquête daadwerkelijk volledig hebben ingevuld. Een aanvulling op de HAIS-Q betreft een extra vraag naar contact met externe partijen zoals leveranciers, tussenpersonen, accountants en verzekeringsmaatschappijen. Deze toevoeging vloeit voort uit een aanbeveling waarop beide groepen e-mailcontact hebben met onbekende afzenders. Tevens is er gekeken of vertrouwen in de technologie invloed heeft op ISA. In hoofdstuk 4.3 is uitgebreid de betrouwbaarheid van X-HAIS-Q besproken, om deze te verhogen zijn in totaal twee items verwijderd, één voor de KAB dimensie Attitude en één voor de KAB dimensie Behavior, dit is gedaan om de minimale waarde van 0,7 te behalen conform de Cronbach’s Alpha. Daarnaast voldeed Kennisdimensie niet aan de aanbevolen Cronbach’s Alpha ondanks er meerdere items zijn verwijderd, hierdoor kunnen geen betrouwbare conclusies getrokken worden uit de Kennisdimensie. Dit betreft hetzelfde resultaat als het onderzoek van (Takens, 2020). Deze beperking kan in toekomstig onderzoek worden voorkomen door de items meer op elkaar aan te laten sluiten zodat de vragen consistenter kunnen worden beantwoord. Desondanks is er een Cronbach’s Alpha op algemeen ISA niveau van 0.765 behaald, dit betreft een lagere interne consistentie dan in onderzoek van (Takens, 2020) waar een .857 Cronbach's Alpha is behaald. Een verklaring hiervoor kan te maken hebben met de acceptatie van een minimumniveau van 0,5 op de verschillende items conform de theorie van (Pallant , 2007). Dit in tegenstelling tot het aanhouden van de waarde van 0,7 conform eerder onderzoek.

Uit de resultaten blijkt dat er gelijk wordt gescoord op algemeen ISA niveau. Zowel de medewerkers van het hoofdkantoor als de medewerkers van een bijkantoor behalen een cijfer van 89. Dit sluit niet aan op resultaat uit eerder onderzoek waarbij een hoger algemeen niveau van ISA is gebleken voor de medewerkers op het hoofdkantoor (Takens, 2020). Een verklaring van dit verschil wordt niet gevonden, er wordt aangeraden om aanvullend onderzoek uit te voeren binnen dezelfde grootbank zodat hier extra validatie op kan plaatsvinden. Hieronder vindt een vergelijking plaats op niveau per aandachtsgebied waarbij gedetailleerd de bevindingen worden vergeleken met eerder onderzoek.

Password Management

Resultaat toont aan dat medewerkers van het hoofdkantoor een hoger ISA niveau scoren dan de medewerkers van een bijkantoor. Dit sluit aan bij eerder onderzoek en valt in de lijn der verwachting. Er is tevens statistisch bewijs gevonden op de stelling: *De houding van medewerkers van de filialen ten opzichte van het gebruik van sterke wachtwoorden is waarschijnlijk lager dan die van de medewerkers van het hoofdkantoor.* Naast het feit dat er lager wordt gescoord op ISA niveau laten de medewerkers van een bijkantoor ook zien dat men lager scoort op houding ten aanzien van het gedrag echter scoren de medewerkers van een bijkantoor wel hoger op ISA dan eerder onderzoek heeft aangetoond. In eerder onderzoek is tevens significant verschil gebleken in de item: 'It's safe to have a work password with just letters' (attitude). Medewerkers van het hoofdkantoor scoorde aanzienlijk hoger op awareness niveau dan de medewerkers van een bijkantoor. Uit dit onderzoek blijkt een hogere waarde op hetzelfde item echter wordt deze niet significant bevonden conform de Mann-Whitney U test. Een verklaring zou kunnen zijn dat er een andere populatie is gebruikt dan eerder onderzoek, dit is een bewuste keuze geweest aangezien op deze manier niet twee keer dezelfde enquête ontvangt. Om de betrouwbaarheid te verhogen en de resultaten te valideren kan er vervolgonderzoek worden uitgevoerd met exact dezelfde enquête.
Daarnaast worden in dit onderzoek de volgende significante verschillen op item niveau gevonden die niet in eerder onderzoek zijn aangetoond:

- It's safe to use the same password for social media and work accounts. De test geeft aan dat medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) beter scoren dan de medewerkers van een bijkantoor. Ofwel: medewerkers van het hoofdkantoor achten het minder veilig om hetzelfde wachtwoord voor zowel een social media, als werkaccount te gebruiken.
- It's a bad idea to share my work passwords, even if a colleague asks for it. De test geeft weer dat de medewerkers van een bijkantoor (op de KAB dimensie Attitude) beter scoren dan de medewerkers van het hoofdkantoor. Ofwel: medewerkers van een bijkantoor achten het minder veilig om een wachtwoord te delen met een collega, zelfs als deze collega er naar vraagt.

Waarom er andere significante verschillen zijn gevonden, met name voor de laatste stelling waarbij medewerkers van een bijkantoor beter scoren dan de medewerkers van het hoofkantoor is lastig verklaarbaar. Om de reden van de significante verschillen te achterhalen kan vervolgonderzoek worden uitgevoerd.

Email Use

Resultaat toont aan dat de medewerkers van een bijkantoor hoger scoren op ISA niveau dan de medewerkers van het hoofdkantoor, er zijn echter geen significante verschillen op item niveau geconstateerd. Dit sluit niet aan bij de verwachtingen vanuit eerder onderzoek (Takens, 2020) waarbij de volgende significante verschillen zijn gemeten:

- I am not permitted to click on a link in an email from an unknown sender. De test gaf op dit item aan dat de bewustwording van de medewerkers van een bijkantoor hoger scoren dan de medewerkers van een hoofdkantoor (op de KAB dimensie Knowledge).
- If an email from an unknown sender looks interesting, I click on a link within it. De test gaf op dit item aan dat bewustzijnsniveaus van de medewerkers op het hoofdkantoor hoger scoren dan de medewerkers van een bijkantoor (op de KAB dimensie Behavior)
- I am allowed to open email attachments from unknown senders. De test gaf op dit item aan dat bewustzijnsniveaus van de medewerkers op het hoofdkantoor hoger scoren dan de medewerkers van een bijkantoor (op de KAB dimensie Knowledge)

De resultaten in het huidige onderzoek laten zien dat er conform de Mann-Whitney U test geen significante verschillen op item niveau te zien is. Bijzonder is, dat deze resultaten dus niet aansluiten op eerder onderzoek van (Takens, 2020). Nieuwe inzichten laten wel zien dat er door de medewerkers van een bijkantoor lager wordt gescoord op item I am not permitted to click on a link in an email from an unknown sender dan de medewerkers op een hoofdkantoor. En de

medewerkers van het hoofdkantoor scoren net als eerder resultaat hoger op items If an email from an unknown sender looks interesting, I click on a link within it en I am allowed to open email attachments from unknown senders. Waarom er net anders wordt gescoord op het eerste item is niet duidelijk. Een veronderstelling uit eerder onderzoek (Takens, 2020) was dat medewerkers van het hoofdkantoor minder contact zullen hebben met externe partijen. Door deze beperkingen uit eerder onderzoek weg te nemen ontdekken we in dit onderzoek de opvallende bevinding dat 17 van de 45 medewerkers van het hoofdkantoor contact heeft met externe partijen tegenover 28 medewerkers van een bijkantoor. Dit is 38% tegen over 62% van de totale populatie en uiteindelijk een verschil van 24%. De combinatie van andere resultaten en nieuwe inzichten geeft weer dat de eerder gestelde conclusie niet direct te herleiden is aan de hoeveelheid externe contacten met aannames tussen verschillen van de medewerkers van het hoofdkantoor of een bijkantoor.

Social Media Use

Resultaat toont aan dat er gelijk wordt gescoord op ISA niveau. Wel laten de medewerkers van een bijkantoor een beter gedrag zien. Daarnaast is er een significant verschil aangetoond op het volgende item: It's risky to post certain information about my work on social media. De test laat zien dat de medewerkers van het hoofdkantoor (op de KAB dimensie Attitude) hoger scoren dan de medewerkers van een bijkantoor. Ofwel: de medewerkers van een bijkantoor vinden het minder risicovol om bepaalde informatie over werk op social media te plaatsen. Dit is een opvallende bevinding ten aanzien van eerdere resultaten, er is namelijk niet eerder een significant verschil op dit item aangetoond. Uit eerder onderzoek zijn er tevens andere significante verschillen gemeten op item niveau:

- It’s a good idea to regularly review my social media privacy settings. De test gaf op dit item aan dat de medewerkers van het hoofdkantoor hoger scoren op houding dan de medewerkers van een bijkantoor.
- I don’t regularly review my social media privacy settings. De test gaf op dit item aan dat de medewerkers van het hoofdkantoor hoger scoren op gedrag dan de medewerkers van een bijkantoor.
- I can’t be fired for something I post on social media. De test gaf op dit item aan dat de medewerkers van het hoofdkantoor hoger scoren op kennis dan de medewerkers van een bijkantoor. Er was geen verschil gemeten op houding en gedrag.

Alle drie de items uit eerder onderzoek verwijzen naar het voordeel van de medewerkers van het hoofdkantoor. De nieuwe inzichten geven geen significant verschil aan, wel is te zien dat de medewerkers van een bijkantoor hoger scoren op het eerste item en er op de tweede en derde items gelijk wordt gescoord. Hierdoor kunnen we met de nieuwe resultaten concluderen dat het verschil tussen de groepen kleiner is dan eerste instantie werd gedacht. Eventueel vervolgonderzoek kan plaatsvinden om te kijken waarom deze specifieke verschillen niet meer aanwezig zijn.

Voor de aandachtsgebieden Mobile Devices en Incident reporting zijn zowel uit eerder onderzoek als huidig onderzoek geen significante verschillen op item niveau aangetoond. Op ISA niveau wordt gelijk gescoord op Mobile Devices en voor Incident reporting scoren de medewerkers van het bijkantoor een punt hoger net als in eerder onderzoek. Dit toont tevens de betrouwbaarheid van het onderzoek aan, de resultaten zijn immers hetzelfde nadat het onderzoek nogmaals is uitgevoerd. Een oorzaak dat tot twee keer toe de medewerkers van een bijkantoor hoger scoren op Incident reporting kan te maken hebben met de aandacht voor het melden van incidenten bij klanten, medewerkers van een bijkantoor hebben immers klantcontact. Dit is tevens te zien aan item: It’s optional to report security incidents. De medewerkers van een bijkantoor scoren hier een stuk hoger dan de medewerkers van het hoofdkantoor. Echter is er geen significant verschil aangetoond door de Mann-Whitney U test waardoor een harde conclusie voorbarig is.

Dit onderzoek kan niet bevestigen of vertrouwen in de technologie verband houdt met gedrag, houding of kennis op ISA. Tijdens het uitvoeren van de statistische toetsen is gebleken dat er geen

causaliteit kan worden aangetoond middels een correlatie. Dit heeft te maken met het lage aantal items (4). De combinatie van weinig empirisch onderzoek en het niet kunnen achterhalen van een causaal verband maakt dat er geen conclusie kan worden gegeven over dit aandachtsgebied. Desondanks heeft het wel nieuwe inzichten weergegeven, om deze beperking in toekomstig onderzoek te voorkomen dient er 1) een uitgebreide analyse plaats te vinden op de items en 2) minimaal 12 items te worden bedacht.

5.2. Conclusies

In het vorige hoofdstuk zijn de resultaten uitgebreid weergegeven, geïnterpreteerd en vergeleken met eerder onderzoek. Daarnaast is er aandacht besteed aan de betrouwbaarheid, validiteit en zijn eventuele beperkingen besproken. Aan de hand van de resultaten is het mogelijk om een conclusie te geven waarbij beantwoording op de hoofdvraag centraal staat: Wat heeft een differentiatie op ISA voor effect op de informatiebeveiliging van hoofd- en bijkantoor?

Uit literatuuronderzoek is gebleken dat ondanks het gebruik van meerdere controles organisaties beveiligingslekken blijven ervaren, er tekortkomingen zijn in bewustwordingsgedrag en beveiligingsbewustzijn van medewerkers de grootste uitdaging betreft. Ook weten we dat het gedrag van medewerkers een cruciale rol speelt in de effectieve informatiebeveiligingsomgeving (Furnell, Sohrabi Safa , & Von Solms , 2016). Uit een onderzoek naar ISA binnen 3 grootbanken bleek dat er differentiatie in groepen is gebruikt vanwege de verschillende IS-risico's en gedrag van medewerkers echter is de inhoud van de differentiatie niet onderzocht Bauer et al. (2017). Dit onderzoek heeft plaatsgevonden middels een opgestelde enquête genaamd de HAIS-Q. Een volgend onderzoek binnen een grootbank in Nederland heeft nieuwe kennis toegevoegd door een verkorte versie van de HAIS-Q op te zetten. Hierin zijn verschillen waargenomen tussen de medewerkers van het hoofdkantoor en een bijkantoor binnen de ISA aandachtsgebieden wachtwoordbeheer, e-mailgebruik en gebruik van sociale media (Takens, 2020). Om enerzijds deze resultaten te valideren en anderzijds nieuwe inzichten te genereren is de kennis uit dit onderzoek als basis gebruikt om de volgende conclusies te kunnen geven. Allereerst werd conform eerder onderzoek een hoger overall ISA niveau verwacht voor de medewerkers van een hoofdkantoor. Een belangrijke bevinding in ons onderzoek betreft een gelijk ISA niveau tussen de twee groepen medewerkers. Daarnaast wordt de theorie bevestigd doordat uit het resultaat blijkt dat medewerkers van het hoofdkantoor een hoger ISA niveau voor het aandachtsgebied wachtwoordbeheer hebben dan de medewerkers van een bijkantoor. Opvallend is wel dat de significante verschillen niet op dezelfde items uit eerder onderzoek zijn geconstateerd. Daarnaast zijn er geen belangrijke verschillen in het aandachtsgebied e-mail gebruik geconstateerd, een beperking uit vorig onderzoek was dat er geen inzicht was in de mate waarin de respondenten contact hadden met onbekende afzenders en de aanname is gedaan dat medewerkers van een bijkantoor vaker contact met onbekende afzenders heeft. Uit ons resultaat blijkt dat 17 van de 45 medewerkers van het hoofdkantoor contact heeft met onbekende afzenders tegenover 28 medewerkers van een bijkantoor. Het aandachtsgebied social media geeft een gelijk niveau van ISA tussen de verschillende groepen weer, daarnaast is er wel een significant verschil geconstateerd op een ander item dan de items op het gebied van social media in eerder onderzoek. Op basis van dit item kan er geconcludeerd worden dat de medewerkers van een bijkantoor het minder risicovol vinden om bepaalde informatie over werk op social media te plaatsen. Met de nieuwe inzichten kan er geconcludeerd worden dat de verschillen tussen de groepen medewerkers binnen grootbank X kleiner zijn dan eerste instantie werd gedacht. Deze conclusie is dan puur gebaseerd op resultaat uit de statistische toetsen waaruit minder significante verschillen op item niveau zijn geconstateerd. Echter is een sample van 60 respondenten te laag om een uitspraak over de gehele populatie te kunnen doen (Lewis, Saunders, & Thornhill, 2019), om de exacte oorzaak van deze verschillen te achterhalen wordt dan ook sterk aangeraden vervolgonderzoek uit te voeren.

5.1. Aanbevelingen voor de praktijk

We weten nu dat inzicht in ISA en de bijbehorende factoren essentieel zijn voor het beperken van informatiebeveiligingsrisico's. Daarnaast zijn leiderschap, cultuur en vertrouwen belangrijke elementen in een organisatie. In het kader van “voorkomen is beter dan genezen” speelt preventie een belangrijke rol, een interactieve benadering en op maat gemaakt ISA programma is conform de theorie effectief. Uit de resultaten is gebleken dat conform de theorie en huidig onderzoek de medewerkers van een bijkantoor lager scoren op ISA aandachtsgebied wachtwoordbeheer. Een concrete aanbeveling is een op maat gemaakt ISA programma met aandacht voor het gebruik van wachtwoorden. Om een link te maken naar de actualiteit wordt de kans groot geacht dat er vaker thuis zal worden gewerkt, verstandig is om het programma hierop aan te passen. Uit de resultaten is geen differentiatie op de kennis en gedrag dimensie gemeten, wel op de houding. Een aanbeveling is dan ook om de focus te houden op de houding van de medewerkers aangezien uit de theorie blijkt dat een juiste houding resulteert in beter gedrag op het gebied van informatiebeveiliging. Een laatste belangrijke bevinding betreft dat er vaker extern contact is waargenomen bij medewerkers van het hoofdkantoor dan in eerste instantie werd gedacht. Of dit uiteindelijk resulteert in een groter risico kan verder uitgezocht worden binnen de organisatie.

5.2. Aanbevelingen voor verder onderzoek

Dit onderzoek resulteert in nieuwe ISA inzichten en eventuele verschillen tussen medewerkers van het hoofdkantoor en medewerkers van een bijkantoor. Echter zijn er contrasterende resultaten waargenomen ten aanzien van de literatuur en eerder uitgevoerd onderzoek. Om de betrouwbaarheid te verhogen is het raadzaam om huidig onderzoek als basis te gebruiken voor vervolgonderzoek met extra aandacht voor de aandachtsgebieden Password Management, Email use en Social media use. Daarnaast zullen de resultaten een hogere generaliseerbaarheid hebben indien hetzelfde onderzoek wordt uitgevoerd binnen een bredere vorm van financiële dienstverlening denk aan verzekeraars, pensioenfondsen etc. Tevens is geconcludeerd dat de verschillen tussen de groepen medewerkers binnen grootbank X kleiner zijn dan eerste instantie werd gedacht. Dit is alleen gebaseerd op resultaat uit de statistische toetsen waaruit minder significante verschillen op item niveau zijn geconstateerd. Om de exacte oorzaak van deze verschillen te achterhalen wordt aangeraden vervolgonderzoek uit te voeren.

Dit onderzoek kan niet bevestigen of vertrouwen in de technologie verband houdt met gedrag, houding of kennis op ISA. Tijdens het uitvoeren van de statistische toetsen is gebleken dat er geen causaliteit kan worden aangetoond middels een correlatie. Desondanks heeft het wel nieuwe inzichten weergegeven, in toekomstig onderzoek wordt aanbevolen om naast de hoeveelheid items tevens een uitgebreide analyse te maken op de nieuwe items omtrent vertrouwen in de technologie. Nieuwe inzichten kunnen vervolgens wordt toegevoegd aan de huidige wetenschap.

Bronnen

Ajzen, I. (2006, 31 juli). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology*, *Volume 32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Algemene Rekenkamer (AR). (2009, december). *Het systeem van toezicht op de stabiliteit van financiële markten; Verkenning; Rapport* (Nr. 32255, nr. 2). Sdu uitgevers. Geraadpleegd op 15 maart 2020, van https://www.parlementairemonitor.nl/9353000

Bada, M., Nurse, J., & Sasse, A. M. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Cyber Security Centre Computer Science*, *2019*, 9–10.Geraadpleegd op 16 maart 2020, van https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 59–60. https://doi.org/10.1145/3130515.3130519

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Bell, J., & Waters, S. (2014). *Doing Your Research Project: A Guide For First-Time Researchers* (6th editie). McGraw-Hill Education.

Berkovsky, S., Chen, F., Conway, D., Harris, M., Taib, R., & Yu, K. (2017). A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing. *Symposium on Usable Privacy and Security*, *July 12-14*, 126–127. Geraadpleegd op 7 maart 2020, van https://www.usenix.org/system/files/conference/soups2017

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009a). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 160–161. https://doi.org/10.1057/ejis.2009.8

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009b). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 386–387. https://doi.org/10.1057/ejis.2009.8

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 548. https://doi.org/10.2307/25750690

Cavusoglu, H., Benbasat, I., & Bulgurcu, B. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Compliance. *European and Mediterranean Conference on Information Systems*, *July 13-14*, 11. Geraadpleegd op 15 maart 2020, van https://conferencealerts.com/

Cheong-Tag, K., Hyeun-Suk, R., & Young, R. (2005, december). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *32*, 394. Geraadpleegd op 15 maart 2020, van http://aisel.aisnet.org/icis2005/32

Clarke, N., Furnell, S., & Sherif, E. (2015, december). *wareness, Behaviour and Culture: The ABC in Cultivating Security Compliance.* 93. https://doi.org/10.1109/ICITST.2015.7412064

Clinebell, S., & Shadwick, G. (2005). The Importance of Organizational Context on Employees' Attitudes: An Examination of Worlking in Main Offices Versus Branch Offices. *Journal of Leadership & Organizational Studies*, *11*(2), 98–99. https://doi.org/10.1177/107179190501100209

Costa, P., & McCrae, R. (1992). Normal personality assessment in clinical practice: The NEO Personality Inventory. *Psychological assessment*, *Vol. 4*, 5–7. Geraadpleegd op 21 maart 2020, van https://550ed48d0cf2ac2905ad119a.pdf

Couper, M. P., Kapteyn, A., Schonlau, M., & Winter, J. (2007). Noncoverage and nonresponse in an Internet survey. *Social Science Research*, *36*(1), 131–148. https://doi.org/10.1016/j.ssresearch.2005.10.002

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and Conducting Mixed Methods Research* (3de editie). SAGE Publications.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Cultures and organizations: software of the mind. (2005). *Choice Reviews Online*, *42*(10), 1–2. https://doi.org/10.5860/choice.42-5937

De Nederlandsche Bank. (2020, april). *Informatiebeveiligingsmonitor* (Nr. 2). Geraadpleegd op 4maart 2020, van https://www.dnb.nl/binaries/WEB_127470_IB_Monitor_tcm46-388405.pdf

de Winter, J., & Dodou, D. (2010). Five-point Likert items: t test versus Mann-Whitney-Wilcoxon. *CiteSeerX*, *Vol. 15*, 1. Geraadpleegd op 11 oktober 2020, van https://scholarworks.umass.edu/pare/vol15/iss1/11

El-Haddadeh, R., Karyda, M., & Tsohou, A. (2012, juni). Implementation challenges for information security awareness initiatives in e-government. In ECIS (Red.), *179* (pp. 9–11). Geraadpleegd op 21 maart 2020, van https://aisel.aisnet.org/ecis2012/179

Fishbein, M., & Ajzen, I. (1981). On construct validity: A critique of Miniard and Cohen's paper. *Journal of Experimental Social Psychology*, *17*(3), 340–342. https://doi.org/10.1016/0022-1031(81)90032-9

Hsu, C., Backhouse, J., & Silva, L. (2014). Institutionalizing Operational Risk Management: An Empirical Study. *Journal of Information Technology*, *29*(1), 59–72. https://doi.org/10.1057/jit.2013.15

Humaidi, N., & Balakrishnan, V. (2013). Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Journal of Health & Medical Informatics*, *04*(02), 316–317. https://doi.org/10.4172/2157-7420.1000123

Humaidi, N., & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. *International Journal of Information and Education Technology*, *5*(4), 311–318. https://doi.org/10.7763/ijiet.2015.v5.522

Information Security Forum. (2002, april). *Effective Security Awareness* (Nr. 1). Geraadpleegd op 4 maart 2020, van https://docplayer.net/1261050-Effective-security-awareness-workshop-report.html

Kam, H. J., Mattson, T., & Goel, S. (2019). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers*, *22*(5), 13–16. https://doi.org/10.1007/s10796-019-09927-9

Kaushal, S. (2011, november). *Effect of leadership and organizational culture on information technology effectiveness: A review*. 4–5. https://doi.org/10.1109/ICRIIS.2011.6125668

Kim, S., & Kim, Y. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 1001–1003. https://doi.org/10.1108/jkm-08-2016-0353

Mani, D., Mubarak , S., & Choo, K.-K., D., Mubarak, S., & Choo, K. K. R. (2014, augustus). *Understanding the Information Security Awareness Process in Real Estate Organizations Using the SECI Mode*. 6–9.

Marshall, P. (2002). Building an Information Security Awareness Program. *Journal of Government Information*, *29*(6), 431–433. https://doi.org/10.1016/j.jgi.2003.12.014

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Mudrack, P. (2007). Individual Personality Factors That Affect Normative Beliefs About the Rightness of Corporate Social Responsibility. *Business & Society*, *46*(1), 33–62. https://doi.org/10.1177/0007650306290312

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 173–174. https://doi.org/10.1016/j.cose.2013.12.003

PwC. (2018, oktober). *Digital Trust Insights*. Geraadpleegd op 28 maart 2020, van https://pwc.com/us/digitaltrustinsights

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Roper, C., Fischer, L., & Grau, J. A. (2005). *Security Education, Awareness and Training: SEAT from Theory to Practice* (1ste editie). Butterworth-Heinemann.

Rousseau, D. M. (1978). Characteristics of Departments, Positions, and Individuals: Contexts for Attitudes and Behavior. *Administrative Science Quarterly*, *23*(4), 521–538. https://doi.org/10.2307/2392578

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7de editie). Pearson Education Limited.

Schoof, D. (2018, juni). *National Cyber Security Research Agenda*. NCSRA III, Amsterdam, Netherlands.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, *32*(2), 729–730. https://doi.org/10.5465/amr.2007.24348410

Schütz, A. (2018). *Information Security Awareness: It's Time to Change Minds!* 1–2.

Scott, R. W. (2007). *Institutions and Organizations: Ideas and Interests* (3rd editie). SAGE Publications, Inc.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 98–99. https://doi.org/10.1108/09685220010371394

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Stake, R. E. (1995). *The Art of Case Study Research* (illustrated edition). Sage Publications, Inc.

Takens, N. (2020, juni). *Information Security Awareness of bank employees: how differences between headquarter and branch employees affect ISA program design.* (Masterscriptie). (Nr. 852061695). Open Universiteit, faculteit Bètawetenschappen. Geraadpleegd op 5 september 2020, van https://research.ou.nl/en/studentTheses/

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 11–12. https://doi.org/10.1057/ejis.2013.27

Yin, R. K. (2017). *Case Study Research and Applications* (6de editie). SAGE Publications.

Bijlage 1 Vereisten/parameters artikelen

De basisprocedures voor het zoeken naar literatuur betreft het bepalen van de parameters van de studie en het verfijnen en focussen van trefwoorden die het mogelijk maken om het identificeren van relevante bronnen en, indien mogelijk, het elimineren van de meeste de irrelevantie.
De volgende parameters komen uit de theorie van Bell,J (Bell, Maidenhead).

- Om foutieve interpretaties te voorkomen is er zoveel mogelijk gebruik gemaakt van Engelstalige artikelen.
- De publicatieperiode betreft artikelen geschreven vanaf 2016. Mede gezien de snelheid van de technologie en achterhaalde informatie is het niet gebruikelijk om een grote hoeveelheid artikelen ouder dan 4 jaar te gebruiken.
- De concentratie van de zoektermen is Information Security Awareness. Dit blijft het hoofdonderwerp gedurende de zoektocht.
- Er wordt alleen gebruik gemaakt van openbaar toegankelijke artikelen.
- Er wordt alleen gebruik gemaakt van wetenschappelijke artikelen

Bijlage 2 HAIS-Q

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. ^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. ^
Considering consequences	I can't be fired for something I post on social media. ^	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. ^
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.^	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. ^	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Bijlage 3 Resultaten Mann-Whitney U test

Password Management

				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNP01	K	It's acceptable to use my social media passwords on my work accounts.	33	33,67	1111,00	29	29,03	842,00	407,000	842,000	-1,079	,280
2.	ATP01	A	It's safe to use the same password for social media and work accounts.	33	34,58	1141,00	28	26,79	750,00	344,000	750,000	-1,900	,057
3.	BEP01	B	I use a different password for my social media and work accounts.	32	30,98	991,50	29	31,02	899,50	463,500	991,500	-,008	,994
4.	KNP02	K	I am allowed to share my work passwords with my colleagues.	33	31,68	1045,50	29	31,29	907,50	472,500	907,500	-,165	,869
5.	ATP02	A	It's a bad idea to share my work passwords, even if a colleague asks for it.	33	28,15	929,00	28	34,36	962,00	368,000	929,000	-2,039	,041
6.	BEP02	B	I share my work passwords with colleagues.	33	29,98	989,50	29	33,22	989,50	428,500	989,500	-1,031	,303
7.	KNP03	K	A mixture of letters, numbers and symbols is necessary for my work passwords.	33	32,67	1078,00	29	30,17	875,00	440,000	875,000	-,622	,534
8.	ATP03	A	It's safe to have a work password with just letters.	33	31,64	1044,00	28	30,25	847,00	441,000	847,000	-,342	,732
9.	BEP03	B	I use a combination of letters, numbers and symbols in my work passwords.	33	29,39	970,00	27	31,85	860,00	409,000	970,000	-,620	,535

Email use

				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNE04	K	I am allowed to click on any links in emails from people I know.	33	29,94	988,00	29	29,94	965,00	427,000	988,000	-,789	,430
2.	ATE04	A	It's always safe to click on links in emails from people I know.	33	30,53	1007,50	28	31,55	883,50	446,500	1007,500	-,255	,799
3.	BEE04	B	I don't always click on links in emails just because they come from someone I know.	33	32,26	1064,50	28	29,52	826,50	420,500	826,500	-,671	,502
4.	KNE05	K	I am not permitted to click on a link in an email from an unknown sender.	32	32,55	1041,50	29	29,29	849,50	414,500	849,500	-,754	,451
5.	ATE05	A	Nothing bad can happen if I click on a link in an email from an unknown sender.	32	32,50	1040,00	28	28,21	790,00	384,000	790,000	-1,177	,239
6.	BEE05	B	If an email from an unknown sender looks interesting, I click on a link within it.	33	32,21	1063,00	29	30,69	890,00	455,000	890,000	-,361	,718
7.	KNE06	K	I am allowed to open email attachments from unknown senders.	33	34,36	1134,00	29	28,24	819,00	384,000	819,000	-1,492	,136
8.	ATE06	A	It's risky to open an email attachment from an unknown sender.	32	30,28	969,00	28	30,75	861,00	441,000	969,000	-,118	,906
9.	BEE06	B	I don't open email attachments if the sender is unknown to me.	33	32,15	1061,00	28	29,64	830,00	424,000	830,000	-,591	,554

Social Media use

				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNS07	K	I must periodically review the privacy settings on my social media accounts.	32	28,36	907,50	29	33,91	983,50	379,500	907,500	-1,294	,196
2.	ATS07	A	It's a good idea to regularly review my social media privacy settings.	31	29,44	912,50	28	30,63	857,50	416,500	912,500	-,300	,764
3.	BES07	B	I don't regularly review my social media privacy settings.	32	29,89	956,50	28	29,89	873,50	428,500	956,500	-,305	,760
4.	KNS08	K	I can't be fired for something I post on social media.	32	33,14	1060,50	29	33,14	830,50	395,500	830,500	-1,041	,298
5.	ATS08	A	It doesn't matter if I post things on social media that I wouldn't normally say in public.	32	31,67	1013,50	28	29,16	816,50	410,500	816,500	-,645	,519
6.	BES08	B	I don't post anything on social media before considering any negative consequences.	31	30,39	942,00	28	29,57	828,00	422,000	828,000	-,213	,831
7.	KNS09	K	I can post what I want about work on social media.	33	29,24	965,00	28	33,07	926,00	404,000	965,000	-1,078	,281
8.	ATS09	A	It's risky to post certain information about my work on social media.	32	35,47	1135,00	28	24,82	695,00	289,000	695,000	-2,625	,009
9.	BES09	B	I post whatever I want about my work on social media.	32	31,06	994,00	29	30,93	897,00	462,000	897,000	-,037	,970

Mobile Devices

				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNM10	K	When working in a public place, I have to keep my laptop with me at all times.	33	32,86	1084,50	29	29,95	868,50	433,500	868,500	-,994	,320
2.	ATM10	A	When working in a café, it's safe to leave my laptop unattended for a minute.	32	30,31	970,00	28	30,71	860,00	442,000	970,000	-,144	,886
3.	BEM10	B	When working in a public place, I leave my laptop unattended.	33	30,00	990,00	29	33,21	963,00	429,000	990,000	-1,016	,310
4.	KNM11	K	I am allowed to send work files via a public Wi-Fi network.	32	31,23	999,50	29	30,74	891,50	456,500	891,500	-,119	,905
5.	ATM11	A	It's risky to send sensitive work files using a public Wi-Fi network.	33	31,42	1037,00	28	30,50	854,00	448,000	854,000	-,224	,823
6.	BEM11	B	I send sensitive work files using a public Wi-Fi network.	32	29,67	949,50	29	32,47	941,50	421,500	949,500	-,677	,498
7.	KNM12	K	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	33	30,85	1018,00	29	32,24	935,00	457,000	1018,000	-,474	,635
8.	ATM12	A	It's risky to access sensitive work files on a laptop if strangers can see my screen.	32	29,69	950,00	28	31,43	880,00	422,000	950,000	-,478	,633
9.	BEM12	B	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	33	33,33	1100,00	29	29,41	853,00	418,000	853,000	-1,007	,314

Incident Reporting

				Hoofdkantoor			Bijkantoor			Testresultaten			
Nr.	Code	KAB	Stelling	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig.
1	KNI13	K	If I see someone acting suspiciously in my workplace, I should report it.	33	31,68	1045,50	28	30,20	845,50	439,500	845,500	-,363	,717
2.	ATI13	A	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	33	32,56	1074,50	28	29,16	816,50	410,500	816,500	-,862	,389
3.	BEI13	B	If I saw someone acting suspiciously in my workplace, I would do something about it.	33	31,85	1051,00	29	31,10	902,00	467,000	902,000	-,195	,846
4.	KNI14	K	I must not ignore poor security behavior by my colleagues.	33	33,32	1099,50	29	29,43	853,50	418,500	853,500	-,908	,364
5.	ATI14	A	Nothing bad can happen if I ignore poor security behavior by a colleague.	33	30,88	1019,00	28	31,14	872,00	458,000	1019,000	-,066	,947
6.	BEI14	B	If I noticed my colleague ignoring security rules, I wouldn't take any action.	33	30,67	1012,00	29	32,45	941,00	451,000	1012,000	-,412	,680
7.	KNI15	K	It's optional to report security incidents.	33	34,17	1127,50	29	28,47	825,50	390,500	825,500	-1,342	,179
8.	ATI15	A	It's risky to ignore security incidents, even if I think they're not significant.	32	32,17	1029,50	28	28,59	800,50	394,500	800,500	-,895	,371
9.	BEI15	B	If I noticed a security incident, I would report it.	33	32,35	1067,50	29	30,53	885,50	450,500	885,500	-,449	,654

Bijlage 4 Resultaten X-HAIS-Q

Hoofdkantoor

Kennis

				Low ISA				High ISA		
				1	2	3	4	5		
Code	Focus area	Question	Reverse coding	Strongly disagree	Disagree	Undecided	Agree	Strongly Agree	Not applicable	Respondents
KNP01	Password management	It's acceptable to use my social media passwords on my work accounts.	Y	14	14	0	4	0	0	31
KNP02	Password management	I am allowed to share my work passwords with my colleagues.	Y	29	2	0	0	0	0	31
KNP03	Password management	A mixture of letters, numbers and symbols is necessary for my work passwords.	N	0	1	0	13	17	0	31
KNE04	Email use	I am allowed to click on any links in emails from people I know.	Y	8	15	2	6	0	0	31
KNE05	Email use	I am not permitted to click on a link in an email from an unknown sender.	N	1	0	6	10	13	1	31
KNE06	Email use	I am allowed to open email attachments from unknown senders.	Y	20	6	3	2	0	0	31
KNS07	Social media use	I must periodically review the privacy settings on my social media accounts.	N	0	6	6	11	7	1	31
KNS08	Social media use	I can't be fired for something I post on social media.	Y	9	11	7	1	2	1	31
KNS09	Social media use	I can post what I want about work on social media.	Y	21	9	0	0	1	0	31
KNM10	Mobile devices	When working in a public place, I have to keep my laptop with me at all times.	N	0	0	0	4	17	0	31
KNM11	Mobile devices	I am allowed to send work files via a public Wi-Fi network.	Y	18	6	3	3	0	0	31
KNM12	Mobile devices	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	N	1	1	0	4	25	0	31
KNI13	Incident reporting	If I see someone acting suspiciously in my workplace, I should report it.	N	0	1	1	15	14	0	31
KNI14	Incident reporting	I must not ignore poor security behavior by my colleagues.	N	2	4	1	13	11	0	31
KNI15	Incident reporting	It's optional to report security incidents.	Y	17	7	2	4	1	0	31

Attitude

				Low ISA				High ISA		
				1	2	3	4	5		
Code	Focus area	Question	Reverse coding	Strongly disagree	Disagree	Undecided	Agree	Strongly Agree	Not applicable	Respondents
ATP01	Password management	It's safe to use the same password for social media and work accounts.	Y	21	6	1	2	1	0	31
ATP02	Password management	It's a bad idea to share my work passwords, even if a colleague asks for it.	N	0	1	0	6	24	0	31
ATP03	Password management	It's safe to have a work password with just letters.	Y	13	14	4	0	0	0	31
ATE04	Email use	It's always safe to click on links in emails from people I know.	Y	10	18	2	1	0	0	31
ATE05	Email use	Nothing bad can happen if I click on a link in an email from an unknown sender.	Y	22	8	0	0	0	1	31
ATE06	Email use	It's risky to open an email attachment from an unknown sender.	N	0	1	1	13	15	1	31
ATS07	Social media use	It's a good idea to regularly review my social media privacy settings.	N	0	0	4	17	8	2	31
ATS08	Social media use	It doesn't matter if I post things on social media that I wouldn't normally say in public.	Y	20	7	1	2	0	1	31
ATS09	Social media use	It's risky to post certain information about my work on social media.	N	0	0	0	12	18	1	31
ATM10	Mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	Y	25	5	0	0	0	1	31
ATM11	Mobile devices	It's risky to send sensitive work files using a public Wi-Fi network.	N	1	1	0	14	15	0	31
ATM12	Mobile devices	It's risky to access sensitive work files on a laptop if strangers can see my screen.	N	0	0	0	11	19	0	31
ATI13	Incident reporting	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Y	17	14	0	0	0	0	31
ATI14	Incident reporting	Nothing bad can happen if I ignore poor security behavior by a colleague.	Y	15	14	0	1	1	0	31
ATI15	Incident reporting	It's risky to ignore security incidents, even if I think they're not significant.	N	1	0	0	15	14	1	31

Behavior										
				Low ISA				High ISA		
				1	2	3	4	5		
Code	**Focus area**	**Question**	**Reverse coding**	**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**	**Not applicable**	**Respondents**
BEP01	Password management	I use a different password for my social media and work accounts.	N	0	7	0	8	15	1	31
BEP02	Password management	I share my work passwords with colleagues.	Y	25	6	0	0	0	0	31
BEP03	Password management	I use a combination of letters, numbers and symbols in my work passwords.	N	0	2	1	11	17	0	31
BEE04	Email use	I don't always click on links in emails just because they come from someone I know.	N	0	2	4	13	12	0	31
BEE05	Email use	If an email from an unknown sender looks interesting, I click on a link within it.	Y	15	9	6	1	0	0	31
BEE06	Email use	I don't open email attachments if the sender is unknown to me.	N	0	1	5	10	15	0	31
BES07	Social media use	I don't regularly review my social media privacy settings.	Y	3	10	6	9	2	1	31
BES08	Social media use	I don't post anything on social media before considering any negative consequences.	N	0	0	1	9	19	2	31
BES09	Social media use	I post whatever I want about my work on social media.	Y	23	7	0	0	0	1	31
BEM10	Mobile devices	When working in a public place, I leave my laptop unattended.	Y	23	6	0	1	1	0	31
BEM11	Mobile devices	I send sensitive work files using a public Wi-Fi network.	Y	16	9	2	3	0	1	31
BEM12	Mobile devices	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	N	0	0	0	11	20	0	31
BEI13	Incident reporting	If I saw someone acting suspiciously in my workplace, I would do something about it.	N	1	2	1	18	9	0	31
BEI14	Incident reporting	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Y	7	16	4	2	2	0	31
BEI15	Incident reporting	If I noticed a security incident, I would report it.	N	0	0	2	16	13	0	31

Trust in Technology										
				Low ISA				High ISA		
				1	2	3	4	5		
Code	**Focus area**	**Question**	**Reverse coding**	**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**	**Not applicable**	**Respondents**
KNT01	Trust	A large majority of the technologies work very well.	N	0	3	5	19	3	1	31
ATT01	Trust	I believe that most technologies allow me to do what I need to do.	N	0	3	9	19	0	1	31
ATT02	Trust	I believe that most technologies are effective in what they should do.	N	0	6	10	11	0	1	31
BET01	Trust	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	N	3	12	5	10	1	0	31
BET02	Trust	Generally, I give a technology the benefit of the doubt when I use it for the first time.	N	5	8	8	9	1	0	31

Bijkantoor

Kennis

				Low ISA				High ISA		
				1	2	3	4	5		
Code	Focus area	Question	Reverse coding	Strongly disagree	Disagree	Undecided	Agree	Strongly Agree	Not applicable	Respondents
KNP01	Password management	It's acceptable to use my social media passwords on my work accounts.	Y	10	11	2	5	1	0	29
KNP02	Password management	I am allowed to share my work passwords with my colleagues.	Y	26	3	0	0	0	0	29
KNP03	Password management	A mixture of letters, numbers and symbols is necessary for my work passwords.	N	0	0	0	16	13	0	29
KNE04	Email use	I am allowed to click on any links in emails from people I know.	Y	10	14	0	3	2	0	29
KNE05	Email use	I am not permitted to click on a link in an email from an unknown sender.	N	0	8	1	9	11	0	29
KNE06	Email use	I am allowed to open email attachments from unknown senders.	Y	13	11	2	3	0	0	29
KNS07	Social media use	I must periodically review the privacy settings on my social media accounts.	N	1	2	3	14	9	0	29
KNS08	Social media use	I can't be fired for something I post on social media.	Y	5	13	4	7	0	0	29
KNS09	Social media use	I can post what I want about work on social media.	Y	22	6	0	0	0	1	29
KNM10	Mobile devices	When working in a public place, I have to keep my laptop with me at all times.	N	0	2	0	4	23	0	29
KNM11	Mobile devices	I am allowed to send work files via a public Wi-Fi network.	Y	15	8	4	1	1	0	29
KNM12	Mobile devices	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	N	1	0	0	3	25	0	29
KNI13	Incident reporting	If I see someone acting suspiciously in my workplace, I should report it.	N	0	1	2	13	12	1	29
KNI14	Incident reporting	I must not ignore poor security behavior by my colleagues.	N	3	5	0	14	7	0	29
KNI15	Incident reporting	It's optional to report security incidents.	Y	12	9	0	4	4	0	29

Attitude

				Low ISA				High ISA		
				1	2	3	4	5		
Code	Focus area	Question	Reverse coding	Strongly disagree	Disagree	Undecided	Agree	Strongly Agree	Not applicable	Respondents
ATP01	Password management	It's safe to use the same password for social media and work accounts.	Y	12	9	2	2	3	1	29
ATP02	Password management	It's a bad idea to share my work passwords, even if a colleague asks for it.	N	0	0	0	2	26	1	29
ATP03	Password management	It's safe to have a work password with just letters.	Y	9	18	0	1	0	1	29
ATE04	Email use	It's always safe to click on links in emails from people I know.	Y	10	15	1	1	1	1	29
ATE05	Email use	Nothing bad can happen if I click on a link in an email from an unknown sender.	Y	17	11	0	0	0	1	29
ATE06	Email use	It's risky to open an email attachment from an unknown sender.	N	0	1	0	12	15	1	29
ATS07	Social media use	It's a good idea to regularly review my social media privacy settings.	N	0	1	3	15	9	1	29
ATS08	Social media use	It doesn't matter if I post things on social media that I wouldn't normally say in public.	Y	16	9	1	1	1	1	29
ATS09	Social media use	It's risky to post certain information about my work on social media.	N	3	0	2	15	8	1	29
ATM10	Mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	Y	24	4	0	0	0	1	29
ATM11	Mobile devices	It's risky to send sensitive work files using a public Wi-Fi network.	N	0	2	1	13	12	1	29
ATM12	Mobile devices	It's risky to access sensitive work files on a laptop if strangers can see my screen.	N	0	0	0	8	20	1	29
ATI13	Incident reporting	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Y	13	15	0	0	0	1	29
ATI14	Incident reporting	Nothing bad can happen if I ignore poor security behavior by a colleague.	Y	12	16	0	0	0	1	29
ATI15	Incident reporting	It's risky to ignore security incidents, even if I think they're not significant.	N	2	1	0	15	10	1	29

Behavior										
				Low ISA				High ISA		
				1	2	3	4	5		
Code	**Focus area**	**Question**	**Reverse coding**	**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**	**Not applicable**	**Respondents**
BEP01	Password management	I use a different password for my social media and work accounts.	N	2	1	0	12	14	0	29
BEP02	Password management	I share my work passwords with colleagues.	Y	25	4	0	0	0	0	29
BEP03	Password management	I use a combination of letters, numbers and symbols in my work passwords.	N	0	2	0	8	17	2	29
BEE04	Email use	I don't always click on links in emails just because they come from someone I know.	N	1	2	0	19	6	1	29
BEE05	Email use	If an email from an unknown sender looks interesting, I click on a link within it.	Y	10	17	0	2	0	0	29
BEE06	Email use	I don't open email attachments if the sender is unknown to me.	N	0	5	0	12	11	1	29
BES07	Social media use	I don't regularly review my social media privacy settings.	Y	2	13	2	10	1	1	29
BES08	Social media use	I don't post anything on social media before considering any negative consequences.	N	0	0	0	12	16	1	29
BES09	Social media use	I post whatever I want about my work on social media.	Y	21	7	0	0	1	0	29
BEM10	Mobile devices	When working in a public place, I leave my laptop unattended.	Y	25	3	0	0	1	0	29
BEM11	Mobile devices	I send sensitive work files using a public Wi-Fi network.	Y	17	7	3	2	0	0	29
BEM12	Mobile devices	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	N	0	1	0	12	16	0	29
BEI13	Incident reporting	If I saw someone acting suspiciously in my workplace, I would do something about it.	N	0	1	0	22	6	0	29
BEI14	Incident reporting	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Y	11	10	0	7	1	1	29
BEI15	Incident reporting	If I noticed a security incident, I would report it.	N	0	1	0	17	11	0	29

Trust in Technology										
				Low ISA				High ISA		
				1	2	3	4	5		
Code	**Focus area**	**Question**	**Reverse coding**	**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**	**Not applicable**	**Respondents**
KNT01	Trust	A large majority of the technologies work very well.	N	3	2	6	16	2	0	29
ATT01	Trust	I believe that most technologies allow me to do what I need to do.	N	0	3	7	17	2	2	29
ATT02	Trust	I believe that most technologies are effective in what they should do.	N	0	3	2	22	0	2	29
BET01	Trust	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	N	0	13	7	9	0	0	29
BET02	Trust	Generally, I give a technology the benefit of the doubt when I use it for the first time.	N	12	4	0	15	1	0	29

Bijlage 5 Vragen X-HAIS-Q

			Algemene vragen	Antwoord
1.			What is your gender?	Male / Female / No answer
2.			What is your age?	18- 25 years / 26-40 / 41-55 / 56-68 / 69+ / no answer
3.			What is the level of school you have completed?	High School / Secundary vocational education (MBO) / Higher professional education (HBO) / University education (WO) / No Answer
4.			Which office do you work for?	Local office / Head office / No answer
5.			Do you have customer contact on a daily basis?	Yes / No
			Focusgebied wachtwoord management	
	KAB	**Onderwerp**		
6.	K	gebruik van het zelfde ww	It's acceptable to use my social media passwords on my work accounts.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
7.	A	gebruik van het zelfde ww	It's safe to use the same password for social media and work accounts	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
8.	B	gebruik van het zelfde ww	I use a different password for my social media and work accounts.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
9.	K	delen van ww	I am allowed to share my work passwords with my colleagues	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
10.	A	delen van ww	It's a bad idea to share my work passwords, even if a colleague asks for it	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
11.	B	delen van ww	I share my work passwords with colleagues	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
12.	K	gebruik van een sterk ww	A mixture of letters, numbers and symbols is necessary for my work passwords	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
13.	A	gebruik van een sterk ww	It's safe to have a work password with just letters	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
14.	B	gebruik van een sterk ww	I use a combination of letters, numbers and symbols in my work passwords.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
			Focusgebied e-mail gebruik	
15.	-	Extra vraag	I regularly receive emails from unknown parties for example customers, suppliers etc.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
16.	K	klikken van linkjes in mails bekend	I am allowed to click on any links in emails from people I know.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
17.	A	klikken van linkjes in mails bekend	It's always safe to click on links in emails from people I know.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
18.	B	klikken van linkjes in mails bekend	I don't always click on links in emails just because they come from someone I know	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
19.	K	klikken van linkjes in mails onbekend	I am not permitted to click on a link in an email from an unknown sender.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
20.	A	klikken van linkjes in mails onbekend	Nothing bad can happen if I click on a link in an email from an unknown sender.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
21.	B	klikken van linkjes in mails onbekend	If an email from an unknown sender looks interesting, I click on a link within it.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
22.	K	Openen van bijlagen in mails onbekend	I am allowed to open email attachments from unknown senders.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
23.	A	Openen van bijlagen in mails onbekend	It's risky to open an email attachment from an unknown sender.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
24.	B	Openen van bijlagen in mails onbekend	I don't open email attachments if the sender is unknown to me.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
			Focusgebied social media	
25.	K	Social media privacy instellingen	I must periodically review the privacy settings on my social media accounts.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
26.	A	Social media privacy instellingen	It's a good idea to regularly review my social media privacy settings.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
27.	B	Social media privacy instellingen	I don't regularly review my social media privacy settings.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
28.	K	overzien van gevolgen	I can't be fired for something I post on social media	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
29.	A	overzien van gevolgen	It doesn't matter if I post things on social media that I wouldn't normally say in public.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
30.	B	overzien van gevolgen	I don't post anything on social media before considering any negative consequences	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
31.	K	prive plaatsen van berichten over werk	I can post what I want about work on social media.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
32.	A	prive plaatsen van berichten over werk	It's risky to post certain information about my work on social media.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
33.	B	prive plaatsen van berichten over werk	I post whatever I want about my work on social media.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
			Focusgebied mobiele apparaten	
34.	K	Fysieke beveiling in openbare ruimte	When working in a public place, I have to keep my laptop with me at all times.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
35.	A	Fysieke beveiling in openbare ruimte	When working in a café, it's safe to leave my laptop unattended for a minute.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
36.	B	Fysieke beveiling in openbare ruimte	When working in a public place, I leave my laptop unattended.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
37.	K	Versturen van gevoelige docs via openbare wifi	I am allowed to send work files via a public Wi-Fi network.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
38.	A	Versturen van gevoelige docs via openbare wifi	It's risky to send sensitive work files using a public Wi-Fi network.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
39.	B	Versturen van gevoelige docs via openbare wifi	I send sensitive work files using a public Wi-Fi network.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
40	K	Meekijken met gevoelige informatie	When working on a sensitive document, I must ensure that strangers can't see my laptop	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
41.	A	Meekijken met gevoelige informatie	It's risky to to access sensitive work files on a laptop if strangers can see my screen	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
42.	B	Meekijken met gevoelige informatie	I check that strangers can't see my laptop screen if I'm working on a sensitive document	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
			Focusgebied incidentenmelding	
43.	K	Melden van opvallend gedrag van collega's	If I see someone acting suspiciously in my workplace, I should report it.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
44.	A	Melden van opvallend gedrag van collega's	I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
45.	B	Melden van opvallend gedrag van collega's	If I saw someone acting suspiciously in my workplace, I would do something about it	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
46.	K	Negeren van opvallend gedrag van collega's	I must not ignore poor security behavior by my colleagues.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
47.	A	Negeren van opvallend gedrag van collega's	Nothing bad can happen if I ignore poor security behavior by a colleague	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
48.	B	Negeren van opvallend gedrag van collega's	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
49.	K	Melden van alle incidenten	It's optional to report security incidents.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
50.	A	Melden van alle incidenten	It's risky to ignore security incidents, even if I think they're not significant.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
51.	B	Melden van alle incidenten	If I noticed a security incident, I would report it.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
			Focusgebied vertrouwen in technologie in het algemeen	
52.	K	Vertrouwen in tecnhologie	A large majority of the technologies work very well.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
53.	A	Vertrouwen in tecnhologie	I believe that most technologies allow me to do what I need to do.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
54.	B	Vertrouwen in tecnhologie	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
55.	B	Vertrouwen in tecnhologie	Generally, I give a technology the benefit of the doubt when I use it for the first time.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable
56.	A	Vertrouwen in tecnhologie	I believe that most technologies are effective in what they should do.	Strongly disagree / Disagree / Undecided / Agree / Strongly agree / Not applicable